

**DIPLOMOVÁ PRÁCE**

Softwarová aplikace pro monitorování  
parametrů v mobilních sítích druhé  
generace pro osobní počítač



Software application for second generation of  
mobile network parameters monitoring by PC

## **Poděkování**

Děkuji vedoucímu diplomové práce Ing. Liboru Michalkovi, Ph.D., akademickému pracovníku Katedry telekomunikační techniky, za vedení a cenné rady při zpracování diplomové práce.

V Soběšovicích 5. května 2010 .....

### **Prohlášení**

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Soběšovicích 5. května 2010 .....

## **Abstrakt**

Z norem pro GSM, obsahujících popis komunikace pomocí AT příkazů pro druhou generaci mobilních telefonů, byly vybrány AT příkazy potřebné pro monitorování parametrů mobilní sítě. Na základě těchto příkazů, je sestaven program AT Monitor GSM. Tento program umožňuje zobrazení a logování parametrů, s možností zpracování do protokolu. Bylo provedeno testování tohoto programu v reálných podmínkách a zpracování protokolu. Dalším výstupem je komentovaný kód programu s podrobným návodem obsluhy a možností úpravy pro využití v laboratorních cvičeních.

## **Abstract**

The At commands required for cellular network monitoring were selected from the GSM standards containing a description of communication using AT commands for the second generation mobile phones. On the basis of these commands AT Monitor GSM program is written. The program allows you to display and log parameters, with the possibility of processing the protocol. The program was tested under real-world conditions, the protocol was processed. There is also a source code with commentary included, along with detailed manual. Adjustment for computer lab exercises is optional.

## **Klíčová slova**

AT Monitor GSM, AT příkazy, BTS, Monitorování parametrů sítě v GSM, Mobilní komunikace, AT modem, Parametry sítě, Primární buňka, Sousední buňky, Identifikační kód buňky, LAC

## **Keywords**

AT Monitor GSM, AT commands, BTS, Monitoring of parameters in GSM network, Mobile Communications, AT modem, Network parameters, Primary cell, Neighboring cells, Cell Identity, LAC

**Seznam zkratek**

MS	<i>Mobile Station</i>	Mobilní stanice
3GPP	<i>3rd Generation Partnership Project</i>	Partnerský projekt třetí generace
ARFCN	<i>Absolute Radio Frequency Channel Number</i>	Absolutní rádiové frekvenční číslo kanálu
AT příkazy	<i>Attention Telephone/Terminal commands</i>	Pozor Telefon/Terminál příkazy
B, BCC	<i>Base Station Color Code</i>	Kód barvy BTS
BA	<i>BCCH Allocation</i>	Umístění řídicího kanálu
BCCH	<i>Broadcast Control Channel</i>	Broadcast řídicího kanálu
BSC	<i>Base Station Controller</i>	Základnová řídicí jednotka
BTS	<i>Base Transceiver Station</i>	Základnová převodní stanice
CI, Cell ID	<i>Cell Identity</i>	Identifikační kód buňky
ETSI	<i>European Telecommunications Standards Institute</i>	Evropský institut pro technické standardy
GSM	<i>Global System for Mobile communications</i>	Globální systém pro mobilní komunikace
CH	<i>Channel</i>	Číslo kmitočtového kanálu
IMEI	<i>International Mobile Equipment Identity</i>	Výrobní (identifikační) číslo mobilního telefonu
IMSI	<i>International Mobile Subscriber Identity</i>	Unikátní číslo přidělené mobilním operátorem pro SIM kartu
LAC	<i>Location Area Code</i>	Kód lokace
LAI	<i>Location Area Identity</i>	Identita místní zóny
MCC	<i>Mobile Country Code</i>	Kód země
MNC	<i>Mobile Network Code</i>	Kód sítě
N, NCC	<i>National Color Code</i>	Kód národní barvy
PDU	<i>Protocol Data Unit</i>	Datový paket
PL	<i>Power Level</i>	Výkonová úroveň pro přenos z mobilu do BTS
RX, RL, RXL	<i>Reception Level</i> [dBm]	Příjmová úroveň
RXAM	<i>RXLevel Access Minimum</i> [dBm]	Minimální příjmová úroveň
S	<i>Serving Cell</i>	Buňka na aktivní pozici
SIM	<i>Subscriber Identity Module</i>	Účastnická identifikační karta
TA	<i>Timing Advance</i>	Časový předstih
TS	<i>Time Slot</i>	Časový slot
TXPWR	<i>Allowed Transmit Power</i> [dBm]	Povolený přenosový výkon

## **OBSAH**

<b>1. Úvod .....</b>	<b>1</b>
<b>2. Problematika monitorování parametrů v GSM.....</b>	<b>2</b>
2.1 NetMonitor.....	2
2.2 Servisní menu.....	2
2.2.1 Idle mode.....	2
2.2.2 Dedicated mode.....	4
2.2.3 Vybrané parametry a shrnutí .....	5
2.3 Aplikace mobilních telefonů s OS pro monitorování sítě.....	8
2.4 AT příkazy pravidla.....	9
2.4.1 AT příkazy můžeme rozdělit do třech skupin: .....	9
2.4.2 Základní pravidla AT příkazu .....	10
2.4.3 Forma AT příkazů a odpovědi .....	10
2.5 Parametry sítě - vybrané AT příkazy .....	11
2.5.1 Skupina AT modem .....	12
2.5.2 Skupina Parametry Sítě.....	14
2.5.3 Skupina Primární Buňka .....	16
2.5.4 Skupina Sousední buňky .....	17
<b>3. Aplikace pro monitorování parametrů v GSM .....</b>	<b>22</b>
3.1 Hardwarové vybavení .....	22
3.2 Softwarové vybavení.....	22
3.2.1 TMS Async32 .....	22
3.3 Aplikace pro monitorování parametrů v GSM.....	23
3.3.1 Aplikace AT Monitor GSM .....	23
3.4 Tvorba aplikace AT Monitor GSM.....	24
3.4.1 Detekované sériové porty.....	24
3.4.2 Komponenta VaComm.....	25
3.4.3 AT Chat.....	26
3.4.4 GSM AT Modem .....	27

3.4.5	Parametry sítě.....	27
3.4.6	Primární Buňka .....	28
3.4.7	Vzorkování.....	28
3.4.8	Výběr souboru operátora.....	28
3.4.9	Identifikovaná BTS .....	28
3.4.10	Sousední buňky .....	29
3.4.11	Logovat .....	29
3.4.12	Procedura ATvypis.....	30
3.4.13	Procedura KontrolaAT .....	30
3.4.14	Procedura KontrolaP .....	30
3.4.15	Procedura KontrolaQ .....	31
3.4.16	Procedura KontrolaBCCH .....	31
3.5	<i>Možnosti rozšíření aplikace AT Monitor GSM .....</i>	<i>31</i>
<b>4.</b>	<b>Testování aplikace v reálných podmínkách.....</b>	<b>33</b>
4.1	<i>Zobrazení parametrů.....</i>	<i>33</i>
4.1.1	Graf – Úrovně signálu.....	34
4.2	<i>Logy.....</i>	<i>34</i>
4.2.1	GSM AT Modem a Parametry Sítě .....	34
4.2.2	Primární Buňka .....	35
4.2.3	Sousední buňky .....	36
4.2.4	AT Chat.....	36
4.3	<i>Protokol.....</i>	<i>37</i>
<b>5.</b>	<b>Závěr .....</b>	<b>38</b>
<b>6.</b>	<b>Literatura.....</b>	<b>39</b>



## **OBRÁZKY**

Obrázek 2.1 První obrazovka servisního menu C35i v Idle mode.....	3
Obrázek 2.2 Druhá obrazovka servisního menu C35i v Idle mode.....	4
Obrázek 2.3 První obrazovka servisního menu C35i v Dedicated mode.....	4
Obrázek 2.4 Druhá obrazovka servisního menu C35i v Dedicated mode.....	5
Obrázek 3.1 Aplikace AT Monitor GSM.....	23
Obrázek 4.1 Test AT Monitor GSM v reálných podmínkách.....	33
Obrázek 4.2 Graf – Úroveň signálu .....	34

## **TABULKY**

Tabulka 2.1 Kód země, sítě a přehled operátorů.....	7
Tabulka 2.2 Základní AT příkazy .....	12
Tabulka 2.3 Rozklad datové části PDU řetězce - sousední buňky.....	18
Tabulka 2.4 Rozklad datové části PDU řetězce – seznam kanálu .....	19
Tabulka 2.5 Převodu číselných hodnot RXLEVEL na úroveň signálu.....	20
Tabulka 2.6 Seznam sousedních buněk C60 interpretace s BCCH.....	21
Tabulka 2.7 Seznam sousedních buněk C35i interpretace s BCCH.....	21
Tabulka 4.1 Logovací soubor Modem.log .....	35
Tabulka 4.2 Logovací soubor BTS.log .....	35
Tabulka 4.3 Logovací soubor Sousedni.log.....	36
Tabulka 4.4 Logovací soubor Chat.log.....	36

## 1. Úvod

Pro amatérské monitorování parametrů sítě se nejčastěji používají mobilní telefony (*Mobile Station*, MS) starších značek, pracujících podle standardů druhé generace. Nejznámější výrobci jsou např. Siemens, Nokia, Ericsson, Motorola, Alcatel. U těchto telefonů je snadno dostupné servisní menu nebo NetMonitor, kde lze jednoduše tyto parametry sledovat. Pro účely dalšího zpracování a dlouhodobého sledování jsou tyto menu nevhodné. Naštěstí většina těchto mobilních telefonů umožňuje komunikaci přes datový kabel s PC pomocí AT příkazů (*Attention Telephone/Terminal commands*). Kdy lze většinu těchto parametrů pomocí HyperTerminálu nebo specializovaného programu zachytávat. Tato komunikace je standardizovaná ETSI (*European Telecommunications Standards Institute*), následně pak doplňovaná a upravovaná skupinou 3GPP (*3rd Generation Partnership Project*). Někteří výrobci mobilních telefonů uveřejnili také Referenční manuál AT příkazů pro jednotlivé druhy MS i s popisem podporovaných ještě nestandardizovaných příkazů. Z možnosti pro připojení k PC lze volit mezi dvěma základními druhy datových kabelů – sériový nebo USB kabel.

Na novější mobilní přístroje s operačním systémem Symbian nebo Windows Mobile, již existují specializované aplikace, které monitorování těchto parametrů umožňují např. CellTrack, Fieldtest. Jsou přizpůsobovány podle požadavků uživatelů a nejčastěji se využívají pro takzvaný „Lov BTS“. Výstupem pak těchto lovců jsou neoficiální seznamy umístění BTS (*Base Transceiver Station*), např. stránky „<http://www.gsmweb.cz/>“ [ 13] nebo s odkazy na mezinárodní „<http://www.senderliste.de/>“. Seznamy z českých stránek využívám i já.

Cílem této práce je vytvořit aplikaci pro monitorování parametry sítě přes PC. Pro realizaci, jsem si zvolil sériový kabel pro modely starších mobilních telefonů Siemens a vývojové prostředí Delphi. Na základě standardu a Referenčního manuálu jsem sestavil přehled zajímavých a potřebných AT příkazů pro monitorování sítě. Tyto budou použity a výsledné odpovědi zobrazeny v mém programu. Předpokládanou vlastností programu je logování zjištěných parametrů z možností dalšího zpracování a odzkoušení v reálných podmínkách. Tento program může být základem pro laboratorní cvičení. Okomentovaný zdrojový kód aplikace bude součástí práce s podrobným návodem.

## 2. Problematika monitorování parametrů v GSM

Jak jsem již uvedl v úvodu, pro monitorování parametrů sítě v GSM (*Global System for Mobile Communications*) lze použít MS starších značek. V této kapitole se zaměřím hlavně na získání parametru sítě se servisního menu a načtení pomocí AT příkazů. Další způsoby zmíním jen okrajově. Důležité parametry servisního menu rozeberu podrobněji. Dále uvedu výčet AT příkazů pro zjišťování parametrů sítě. Seznámím s jejich popisem a praktickým využitím. Uvedené parametry jsou získané z mobilního přístroje Siemens C35i popřípadě C60, které použiji i pro tvorbu a test mého programu.

### 2.1 NetMonitor

Pro monitorování sítě pomocí starších mobilních přístrojů Nokia je určena položka menu, která lze aktivovat přes datový kabel. Pod názvem NetMonitor je skryto servisní menu určené především servisním technikům a případně k opravám mobilního přístroje. Údaje uvedené v tomto menu se týkají komunikace mezi mobilním telefonem a základnovou stanicí a interními parametry mobilu. Podrobný popis pro telefony Nokia lze jednoduše nalézt na internetových stránkách. Já se nebudu tímto nástrojem, dále zabývat neboť pro mou práci používám přístroj Siemens.

### 2.2 Servisní menu

Starší mobilní přístroje Siemens, umožňují zobrazit servisní menu. Na internetu lze nalézt aktivační kód nebo program pro zpřístupnění zobrazení tohoto menu. V mém případě jsem aktivoval menu u Siemens C35i kódem. U dalšího testovaného přístroje Siemens C60 nebylo servisní menu aktivováno. Proto budu při popisu vycházet ze staršího typu C35i. Pro můj účel postačí jen část servisního menu „Monitor“, z toho důvodu mám aktivované takzvané malé servisní menu.

Popis vychází s podrobnějšího popisu na internetových stránkách autora „GASBAG“ [ 10] a článkách uveřejněných na „mobil.cz“ [ 11]. Servisní menu „Monitor“ je rozděleno do dvou částí - Pasivní (*Idle mode*) a Aktivní (*Dedicated mode*).

#### 2.2.1 Idle mode

Mód Idle [ 10], [ 11] je klidový stav mobilního přístroje, který je připojen do sítě GSM, ale neprovádí žádnou akci (přenos hlasu, dat atd.).

**Parametry: První obrazovka**

- CH** Číslo kmitočtového kanálu (*Channel*)
- RX** Příjmová úroveň (*Reception Level*) [dBm]
- CI** Identifikační kód buňky (*Cell Identity*)
- C1** Path-loss kritérium; Typ SIM
- LAI** Identita místní zóny (*Location Area Identity*)
  - MCC** Kód země (*Mobile Country Code*)
  - MNC** Kód sítě (*Mobile Network Code*)
  - LAC** Kód lokace (*Location Area Code*)

<b>CH</b> 048	<b>RX</b> -79
<b>CI</b> 6C49	<b>C1</b> +27 B3
<b>LAI</b> 32F020	06B2
<b>TXPWR</b> 33	<b>RXAM</b> -106
<b>C2</b> +28	<b>BSPA</b> 2 <b>BA</b> 15
<b>P0</b>	<b>P1</b>
<b>P2</b>	<b>P3</b>

Obrázek 2.1 První obrazovka servisního menu C35i v Idle mode

- TXPWR** Povolený přenosový výkon (*Allowed Transmit Power*) [dBm]
- RXAM** Minimální příjmová úroveň (*RXLevel Access Minimum*) [dBm]
- C2** Cell-reselection kritérium
- BA** Umístění řídicího kanálu (*BCCH Allocation*)
- BSPA** Multiframe je vlastnost sítě, určující jak často se mobil musí přepínat na příjem
- P0, P1, P2, P3** Paging

**Parametry: Druhá obrazovka**

- CH** Číslo kmitočtového kanálu (*Channel*)
- RL** Příjmová úroveň (*Reception Level*) [dBm]
- C1** Path-loss kritérium; síla signálu vztažená k RXAM
- C2** Cell-reselection kritérium; údaj rozhodující o umístění buňky na aktivní pozici
- N** Kód národní barvy (*National Color Code*)
- B** Kód barvy BTS (*Base Station Color Code*)

CH	RL	C1	C2	NB
S082	85	+21	+21	54
1047	84	+22	+22	51
2088	96	+10	+10	15
3043	99	+07	+07	51
4093	03	+03	+03	50
5084	05	+01	+01	12
6000	00	+00	+00	00

Obrázek 2.2 Druhá obrazovka servisního menu C35i v Idle mode

**S** Buňka na aktivní pozici (*Serving Cell*)

**1–6** Nejsilnější sousední buňky (*Neighbor Cell*)

### 2.2.2 Dedicated mode

Mód Dedicated [ 10], [ 11] je stav mobilního přístroje, při kterém se provádí nějaká akce. Posílá SMS, přenáší se hovor nebo je zprostředkován přenos dat.

**Parametry:** *První obrazovka*

**000** Číslo běžného hovorového kanálu

**TS** Časový slot (*Time Slot*)

**TA** Časový předstih (*Timing Advance*)

**PL** Výkonová úroveň pro přenos z mobilu do BTS (*Power Level*)

**RX** Příjmová úroveň běžného hovorového kanálu (*Reception Level*) [dBm]

**CI** Identifikační kód buňky (*Cell Identity*)

000	TS2	TA00	PL13
RX-079	CI6C49	S0	
C0 045	RX-079	F2	
LF26LS21	QF0QS0		
LAI32F02006B2			
P0	P1		
P2	P3		

Obrázek 2.3 První obrazovka servisního menu C35i v Dedicated mode

**S** Synchronizační burst  
**C0** Číslo řídicího kmitočtového kanálu  
**RX** Příjmová úroveň (*Reception Level*) [dBm]  
**F2** Kódovací algoritmus (*Coding algorithm*)  
**LF** Hodnota C1 při plynulém přenosu z BTS  
**LS** Hodnota C1 při přerušovaném přenosu z BTS  
**QF** Kvalita spojení při plynulém přenosu z BTS  
**QS** Kvalita spojení při přerušovaném přenosu z BTS  
**LAI** Identita místní zóny (*Location Area Identity*)  
**P0, P1, P2, P3** Paging

**Parametry:** *Druhá obrazovka*

**CH** Číslo kmitočtového kanálu (*Channel*)  
**RXL** Příjmová úroveň (*Reception Level*) [dBm]  
**NCC** Kód národní barvy (*National Color Code*)  
**BCC** Kód barvy BTS (*Base Station Color Code*)  
**S** Buňka na aktivní pozici (*Serving Cell*)  
**1–6** Nejsilnější sousední buňky (*Neighbor Cell*)

	CH	RXL	NCC	BCC
<b>S</b>	082	85	5	4
<b>1</b>	047	84	5	1
<b>2</b>	088	96	1	5
<b>3</b>	043	99	5	1
<b>4</b>	093	03	5	0
<b>5</b>	084	05	1	2
<b>6</b>	000	00	0	0

Obrázek 2.4 Druhá obrazovka servisního menu C35i v *Dedicated mode*

### 2.2.3 Vybrané parametry a shrnutí

Pro mou práci je výchozí režim Idle. Mode Dedicated zobrazuje většinu parametry, stejné jako v režimu Idle, jen je doplňuje o parametry související s hovorem nebo přenosem dat. Parametry, které je zajímavé sledovat s pohledu sítě v servisním menu, uvádím níže.

**Parametry sítě****CH – Číslo kmitočtového kanálu (*Channel*)**

GSM 900 [ 8] je přiděleno kmitočtové pásmo 890 MHz až 960 MHz. Obsahuje 124 duplexních radiových kanálů číslovaných od 1 do 124. Každý radiový kanál má šířku 200 kHz. Odstup *uplink* od *downlink* je 45 MHz. Frekvenci nosné lze určit pro *uplink*  $f_{CHup}(n)$  a *downlink*  $f_{CHdl}(n)$ . Kde  $n = \text{ARFCN}$  (*Absolute Radio Frequency Channel Number*) a odpovídá číslu radiového kanálu ze vztahů

$$f_{CHup}(n) = 890,0 + 0,2 \cdot n \quad [\text{MHz}], \quad (2.1)$$

$$f_{CHdl}(n) = f_{CHup}(n) + 45 \quad [\text{MHz}]. \quad (2.2)$$

GSM 1800 [ 8] používá kmitočtové pásmo 1710 MHz až 1880 MHz. V tomto pásmu je umístěno 374 radiových duplexních kanálů, každý šířky 200 kHz. Odstup mezi *uplink* a *downlink* je nyní 95 MHz. Kmitočty nosných se nyní určí ze vztahů

$$f_{CHup}(n) = 1710,0 + 0,2 \cdot (n - 511) \quad [\text{MHz}], \quad (2.3)$$

$$f_{CHdl}(n) = f_{CHup}(n) + 95 \quad [\text{MHz}]. \quad (2.4)$$

**RX – Příjmová úroveň (*Reception Level*)**

Hodnota přijatého výkonu, který měří mobilní stanice. Měření zisku vychází z radiokomunikační rovnice

$$P_p = P_v - L_0 + G_v + G_p \quad [\text{dBm}], \quad (2.5)$$

kde  $P_p$  odpovídá značce RX a je přijímaný výkon [dBm],  $P_v$  vysílací výkon [dBm],  $G_p$  zisk přijímací antény [dBi],  $G_v$  výkon vysílací antény [dBi],  $L_0$  ztráty ve volném prostoru.



**CI – Identifikační kód buňky (*Cell Identity*)**

Cell ID [ 8] je identifikační číslo přiřazené mobilním operátorem buňce v síti, které slouží pro určení přístupového bodu mobilního zařízení. Poloha všech základnových stanic vytváří buňkovou strukturu. Buňky pohybujících se do 50 m se nazývají pikobuňky a používají se pro místa s vysokou koncentrací uživatelů. Mikrobunčky mají poloměr do 1 km a používají se pro oblasti s větším provozem. Makrobunčky se používají pro oblasti s malou hustotou provozu a mají poloměr až desítek kilometrů. Mobilní zařízení v praxi přijímá signál od více základnových stanic.

**LAI – Identita místní zóny (*Location Area Identity*)**

Území pod kontrolou jednoho veřejného mobilního operátora má svůj vlastní jedinečný identifikátor, který je značen jako Identita místní zóny (LAI) [ 9]. Tento mezinárodně jednoznačný identifikátor se skládá, ze tří číslic kódu země (MCC), dvou až tří číslic kódu mobilní sítě operátora (MNC) a kód zóny (LAC), který má až 5 číslic. LAI se vysílá pravidelně v Broadcast kanálu (BCCH, *Broadcast Control Channel*). Mobile stanice LAI ukládá na Subscriber Identity Module (SIM).

**MCC – Kód země (*Mobile Country Code*); MNC – Kód sítě (*Mobile Network Code*)**

Pro českou republiku jsou určené kódy. Uvádím je níže v tabulce pro jednotlivé operátory [ 9].

MCC	MNC	Operátor	Provozovatel	Pásmo [MHz]	Poznámka
230	01	T-Mobile	T-Mobile Česká republika	GSM 900 / GSM 1800 / UMTS 2100	Bývalý Paegas
230	02	O <sub>2</sub>	Telefónica O2 Česká republika	GSM 900 / GSM 1800 / UMTS 2100	Bývalý Eurotel
230	03	Vodafone	Vodafone Česká republika	GSM 900 / GSM 1800 / UMTS 2100	Bývalý Oskar
230	04	U:fon	MobilKom, a.s.	CDMA 410 až 430	
230	98		SŽDC s.p.	GSM-R 900	Železniční komunikace
230	99	Vodafone	Vodafone Česká republika	Testovací	R&D Centre at FEE, CTU

Tabulka 2.1 Kód země, sítě a přehled operátorů

**LAC – Kód zóny (Location Area Code)**

Kód zóny označuje soubor základnových stanic, které jsou seskupeny pro optimální signalizaci. Typicky je to 10 nebo dokonce až 100 základnových stanic (BTS), které sdružuje jedna základnová řídicí jednotka (*Base Station Controller*, BSC). Každá taková zóna má jedinečné identifikační číslo LAC. Toto číslo je vysíláno jako předčísli pro identifikaci základnové stanice.

**S – Buňka na aktivní pozici (*Serving Cell*)**

Buňka na aktivní pozici [ 11], je ta buňka, se kterou zrovna komunikuje mobilní přístroj. První obrazovka servisního menu (*Obrázek 2.1, Obrázek 2.3*) se vztahuje k tomuto řádku. Buňka je území pokryté signálem vysílače BTS a je rozdělena na několik logických sektorů.

**1-6 – Nejsilnější sousední buňky (*Neighbor Cell*)**

Seznam šesti nejsilnějších sousedních slyšitelných buněk [ 11], který je vysílán buňkou na aktivní pozici (*Neighbors list*).

**CH – Číslo kmitočtového kanálu (*Channel*)**

**RXL (RL) – Příjmová úroveň (*Reception Level*)**

Popis těchto parametrů je uveden na začátku kapitoly 2.2.3.

**NCC – Kód národní barvy (*National Color Code*)**

**BCC – Kód barvy BTS (*BTS Color Code*)**

Tyto kódy umožňují rozlišovat buňky pracující na stejném kanále. BCC odlišuje buňky stejné sítě a NCC buňky operátora různých zemí v příhraničních oblastech [ 13]. Dnes jsou však GSM sítě natolik husté, že se musí používat celá dostupná sada kódů tj. 0-7. Pomocí LAC, BCC, NCC a kanálu lze danou buňku jednoznačně identifikovat, pokud není dostupné Cell ID.

## **2.3 Aplikace mobilních telefonů s OS pro monitorování sítě**

Mobilní přístroje obsahující OS umožňují monitorovat parametry pomocí speciálních programů.

### **CellTrack**

Pro operační systém Symbian je nejznámější program CellTrack. Umožňuje zobrazovat parametry sítě, umístění nalezených BTS, doplňovat fotky k BTS a další popisy, vytvářet a pracovat s logy. Zobrazované parametry, odpovídají z větší části parametrům popsaným výše v kapitole 2.2 Servisní menu.

### **Fieldtest**

Je určen pro systém Symbian a obdoba i pro Windows Mobile. Tento program má podobné vlastnosti jako CellTrack.

Podrobnější popis těchto dvou zmiňovaných programů je uveden například na stránkách „<http://www.gsmweb.cz/>“ [ 13]. Nejsou to jediné aplikace umožňující sledovat síť GSM. Na internetu je těchto aplikací celá spousta, jak profesionálních tak i amatérských.

## **2.4 AT příkazy pravidla**

AT příkazy jsou známy také pod Hayes AT příkazy. Různé telefony podporují různé sady příkazů. To znamená, že konkrétní telefon nemusí podporovat všechny AT příkazy a výrobce naopak může rozšířit sadu o jím používané příkazy. V současné době neexistuje směrodatný seznam dostupných AT příkazů všech telefonů. Příkazy přes modem umožňují dávat pokyny jak mobilním telefonním přístrojům, tak i některým běžným telefonům.

Pro použití AT příkazu v mobilní technice pro druhou generaci GSM sítí byly vydány organizací ETIS normy „AT command set for GSM Mobile Equipment (ME); (GSM 07.07 version 7.4.0 Release 1998)“ [ 1] a „Equipment (DTE - DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS); (GSM 07.05 version 5.5.0)“ [ 2]. Většina výrobců pro své typy mobilních telefonů rozšiřuje příkazovou sadu o své AT příkazy, a proto někdy uveřejňují ke svým výrobkům referenční manuály, například k Siemensu: „Manual Reference AT Command Set (GSM 07.07, GSM 07.05, Siemens specific commands) for the SIEMENS Mobile Phones S35i, C35i, M35i“ [ 3].

### **2.4.1 AT příkazy můžeme rozdělit do třech skupin:**

*Základní AT příkazy* – tyto příkazy jsou považovány za standardní výbavu modemu a jsou k dispozici na téměř všech modemech.

*Rozšířené AT příkazy* – jsou příkazy, kdy po „AT“ následuje znak &. Tyto příkazy jsou všeobecně uznávané.

*Proprietární AT příkazy* – tyto příkazy se liší výrobce od výrobce a dokonce i mezi různými modely stejného výrobce.

### 2.4.2 Základní pravidla AT příkazu

AT příkazy musí dodržovat několik základních uzancí, viz [ 12].

- Každý příkaz začíná „AT“ nebo „at“. Kombinace „At“ nebo „aT“ nejsou platné začátky příkazu. Výjimku tvoří příkaz „A/“ opakování a příkaz „+++“ přechod do režimu dat.
- Příkazy mohou být velkými nebo malými písmeny (nekombinovat).
- Několik příkazů lze spojit do jednoho řetězce.
- Délka příkazové řádky by neměla přesáhnout čtyřicet znaků.
- Aby byla možno editovat příkazový řádek, je třeba nejprve backspace smazat předchozí zadané znaky.
- Každý příkaz začínající na „AT“ nebo „at“ musí být ukončen <Enter>, výjimku tvoří jen „+++“ a „A/“.
- Telefonní čísla mohou obsahovat znaky „1“, „2“, „3“, „4“, „5“, „6“, „7“, „8“, „9“, „\*“, „=“, „,“, „;“, „#“, „+“ a „>“. Všechny jiné znaky jsou ignorovány.
- Příkazy s číselnými hodnotami lze použít bez této hodnoty. V tomto případě se dosadí nula.
- Pokud příkazový řetězec obsahuje 2 krát po sobě příkaz bez hodnoty modem zahlásí chybu.
- Po příkazu ATZ by měla nastat 2 sekundová pauza před dalším příkazem z důvodu restartu modemu.

### 2.4.3 Forma AT příkazů a odpovědi

Podle GSM 07,07 a GSM 07,05, je možné provést příkazy AT v různých formách [ 3].

**Testovací příkaz**      AT+CXXX=?

Odpovědí telefonu je zaslání parametrů a rozsahu jejich hodnot, které lze nastavit pomocí přidružených příkazů nebo interních procesů.

**Příkaz pro výčet**      AT+CXXX?

Odpovědí je aktuální hodnota nastavení nebo výčet hodnot.

**Příkaz nastavení**      AT+CXXX=<...>

Tento příkaz se používá pro nastavení parametrů.

**Příkaz proved'**      AT+CXXX

Příkaz spouští neparametrické příkazy, které ovlivňují vnitřní procesy telefonu.

**Pomocné znaky** [ 1 ] pro popis formátování a provádění

<CR>    Znak odřádkování, pokud není uveden parametr.

<LF>    Znak odřádkování, který potvrzuje příkaz zadány s hodnotami.

<...>    Hodnota uzavřená v špičatých závorkách je název parametru. Závorky samy o sobě nejsou uvedeny v příkazovém řádku.

[...]    Volitelné subparametry příkazu nebo volitelná součást odpovědi jsou uzavřeny v hranatých závorkách. Závorky samy o sobě nejsou uvedeny v příkazovém řádku. Není-li subparametr uveden v příkazu, jejich hodnota se rovná předchozí hodnotě. V prováděcích příkazech by měly být hodnoty nastaveny na základě doporučení.

**underline**    Zdůrazněná hodnota subparametru je doporučené výchozí nastavení. Tyto hodnoty by měly zůstat nastaveny podle továrního nastavení, které je konfigurováno dle V.25ter Command &F0. V prováděcích příkazech, je tato hodnota použita, pokud není subparametr zadán.

## 2.5 Parametry sítě - vybrané AT příkazy

Pro mé potřeby jsem vybral příkazy, které souvisejí se zjišťováním parametrů sítě nebo identifikují modem monitorující tyto parametry. Příkazy jsem vybíral s referenčního manuálu „Manual Reference AT Command Set for the SIEMENS Mobile Phones S35i, C35i, M35i” [ 3]. Definici srovnávám s normami ETSI GSM viz literatura [ 1], [ 2]. Jednotlivé definice příkazů

uvádím podle překladu z referenčního manuálu. Příkazy jsou testovány na mobilních přístrojích značky SIEMENS C35i a C60, přes program HyperTerminál. Reakce na AT příkazy uvádím pod každou definicí. Jednotlivé sady AT příkazů rozdělují do kapitol (sdružuji do skupin) podle funkcionality.

### Základní AT příkazy (Hayes) - použité

Příkaz	Funkce	Odpověď
AT	Prefix všech příkazů – vyvolává odpověď	OK
ATE0	Vypíná opakování výpisu při zobrazení odpovědi	OK
ATE1	Zapíná opakování výpisu při zobrazování odpovědi	OK
ATZ	Resetuje modem do defaultního nastavení	OK

Tabulka 2.2 Základní AT příkazy

### 2.5.1 Skupina AT modem

Tímto výčtem parametrů je identifikován modem a SIM karta obou mobilních přístrojů. Pro další použití budu tyto AT příkazy chápat jako jednu skupinu. Výčet příkazu jsem čerpal z literatury [ 1] a [ 3].

#### Dotaz na značku výrobce – AT+CGMI

Testovací příkaz:	AT+CGMI=?	Odpověď:	OK
Prováděcí příkaz:	AT+CGMI	Odpověď:	<Výrobce>
SIEMENS C35i:	AT+CGMI	Odpověď:	SIEMENS
SIEMENS C60:	AT+CGMI	Odpověď:	SIEMENS

#### Dotaz na typ modelu – AT+CGMM

Testovací příkaz:	AT+CGMM=?	Odpověď:	OK
Prováděcí příkaz:	AT+CGMM	Odpověď:	<Model>

---

<i>SIEMENS C35i:</i>	<i>AT+CGMM</i>	<i>Odpověď:</i>	<i>C35i</i>
----------------------	----------------	-----------------	-------------

<i>SIEMENS C60:</i>	<i>AT+CGMM</i>	<i>Odpověď:</i>	<i>C60</i>
---------------------	----------------	-----------------	------------

**Dotaz na verzi firmware - AT+CGMR**

Testovací příkaz:	AT+CGMR=?	Odpověď:	OK
-------------------	-----------	----------	----

Prováděcí příkaz:	AT+CGMR	Odpověď:	<Verze>
-------------------	---------	----------	---------

<i>SIEMENS C35i:</i>	<i>AT+CGMR</i>	<i>Odpověď:</i>	<i>18</i>
----------------------	----------------	-----------------	-----------

<i>SIEMENS C60:</i>	<i>AT+CGMR</i>	<i>Odpověď:</i>	<i>27</i>
---------------------	----------------	-----------------	-----------

**Dotaz na sériové číslo (IMEI) - AT+CGSN (AT+GSN)**

Testovací příkaz:	AT+CGSN=?	Odpověď:	OK
-------------------	-----------	----------	----

Prováděcí příkaz:	AT+CGSN	Odpověď:	<sn>
-------------------	---------	----------	------

<i>SIEMENS C35i:</i>	<i>AT+CGSN</i>	<i>Odpověď:</i>	<i>449191370694883</i>
----------------------	----------------	-----------------	------------------------

<i>SIEMENS C60:</i>	<i>AT+CGSN</i>	<i>Odpověď:</i>	<i>351944000765952</i>
---------------------	----------------	-----------------	------------------------

**Dotaz na SIM ID (IMSI) - AT+CIMI**

Testovací příkaz:	AT+CIMI=?	Odpověď:	OK
-------------------	-----------	----------	----

Prováděcí příkaz:	AT+CIMI	Odpověď:	<imsi>
-------------------	---------	----------	--------

<i>SIEMENS C35i:</i>	<i>AT+CIMI</i>	<i>Odpověď:</i>	<i>230020700935654</i>
----------------------	----------------	-----------------	------------------------

<i>SIEMENS C60:</i>	<i>AT+CIMI</i>	<i>Odpověď:</i>	<i>230014100380921</i>
---------------------	----------------	-----------------	------------------------

**Dotaz na Číslo SIM - AT^SCID Příkaz není uveden v GSM 07.07 [ 1].**

Testovací příkaz:	AT^SCID=?	Odpověď:	OK/ERROR/+CME ERROR
-------------------	-----------	----------	---------------------

Prováděcí příkaz:	AT^SCID	Odpověď:	<cid>
-------------------	---------	----------	-------

<i>SIEMENS C35i:</i>	<i>AT^SCID</i>	<i>Odpověď:</i>	<i>8942020399603556587</i>
----------------------	----------------	-----------------	----------------------------

<i>SIEMENS C60:</i>	<i>AT^SCID</i>	<i>Odpověď:</i>	<i>8942001104138902154</i>
---------------------	----------------	-----------------	----------------------------

Výsledné hodnoty těchto příkazů se v průběhu času nemění, proto nemá smysl při změně hodnoty znova ověřovat. Pouze Číslo SIM nemusí být někdy načtené celé.

### 2.5.2 Skupina Parametry Sítě

Tato skupina příkazů viz [ 1], [ 3] identifikuje operátora a lokalitu, kterou sdružuje základnová řídicí jednotka (BSC).

#### Příkaz týkající se výběru operátora sítě – AT+COPS

Testovací příkaz: AT+COPS=?

Odpověď: (výčet <stat>, dlouhý/krátký název <oper>,  
číslo <oper>)] [, (výčet <mode>), (výčet <format>)]

Výčtový příkaz: AT+COPS?

Odpověď: [<mode>[, <format>[, <oper>]]]

Nastavovací příkaz: AT+COPS=[<mode>[, <format> [, <oper>]]]

Parametry:	<stat>	0	Neznáme
		1	Dostupné
		2	Aktuální
		3	Zakázané
	<oper>		Operátor ve formátu podle <mode>
<mode>		0	Automatický mód (pole <oper> je ignorováno)
		1	Manuální (pole <oper> musí být přítomné)
		2	Odhlášení ze sítě
		3	Nastavení <format> (pro výčet + COPS?)
<format>		4	Automatické / Manuální nastavení
		0	Dlouhý formát názvu <oper>
		1	Krátký formát názvu <oper>
		2	Číselný formát <oper>

<i>SIEMENS C35i:</i>	<i>Nastavení</i>	<i>AT+COPS=3,0</i>	<i>Odpověď: OK</i>
	<i>Výčet</i>	<i>AT+COPS?</i>	<i>Odpověď: 0,0,"EUROTEL -CZ"</i>
	<i>Nastavení</i>	<i>AT+COPS=3,2</i>	<i>Odpověď: OK</i>
	<i>Výčet</i>	<i>AT+COPS?</i>	<i>Odpověď: 0,2,"23002"</i>



---

<i>SIEMENS C60:</i>	<i>Nastavení</i>	<i>AT+COPS=3,0</i>	<i>Odpověď: OK</i>
	<i>Výčet</i>	<i>AT+COPS?</i>	<i>Odpověď: 0,0,"T-Mobile CZ"</i>
	<i>Nastavení</i>	<i>AT+COPS=3,2</i>	<i>Odpověď: OK</i>
	<i>Výčet</i>	<i>AT+COPS?</i>	<i>Odpověď: 0,2,"23001"</i>

**Příkaz týkající se registrace do sítě – AT+CREG**

Testovací příkaz: AT+CREG=?      Odpověď: (výčet <n>)

Výčtový příkaz: AT+CREG?      Odpověď: <n>,<stat>[,<lac>,<ci>]

Nastavovací příkaz: AT +CREG=<n>

Parametry:	<n>	0	Potlačení stavových správ sítě
		1	Zobrazení stavových správ sítě
		2	Umožní síti registraci a informaci o poloze
	<stat>	0	Není registrovaná, nevyhledává
		1	Registruje, domácí síť
		2	Není registrovaná, vyhledává
		3	Registrace odmítnuta
		4	Neznáma
		5	Registrovaná, roaming
	<lac>		Identita místní zóny
	<ci>		Identifikační kód buňky

<i>SIEMENS C35i:</i>	<i>Nastavení</i>	<i>AT+CREG=0</i>	<i>Odpověď: OK</i>
	<i>Výčet</i>	<i>AT+CREG?</i>	<i>Odpověď: 0,1,"06B9","1C17"</i>
<i>SIEMENS C60:</i>	<i>Nastavení</i>	<i>AT+CREG=2</i>	<i>Odpověď: OK</i>
	<i>Výčet</i>	<i>AT+CREG?</i>	<i>Odpověď: 2,1,"7050","A21E"</i>

Popis operátora a kód země, lze získat z tabulky uvede výše (Tabulka 2.1). Jsou v ní uvedené oba formáty, alfanumerický i číselný s prefixem kódu země. V této skupině zjišťují i kód lokace (LAC), do které se mobilní telefonní přístroj registroval. Je udána jedinečným hexadecimálním číslem zvoleným operátorem (první hodnota v uvozovkách), popřípadě po převodu decimálním. Identifikátor určuje základnovou řídicí jednotku (BSC). V této skupině se získá i hodnota kódu buňky (Cell ID), která spadá již do skupiny Primární Buňka (kapitola 2.5.3).

Operátor se může změnit mimo oblast pokrytí nebo v zahraničí, proto je třeba v určených časových intervalech hodnoty kontrolovat.

### 2.5.3 Skupina Primární Buňka

Tato skupina uvádí identifikátory primární buňky a sílu signálu [ 1], [ 3] přijímanou z této buňky mobilním přístrojem.

#### Příkaz týkající se registrace do sítě - AT+CREG

Pro načtení parametrů po registraci do sítě platí pravidla uvedená v části kapitoly 2.5.2. Identifikátor kódu buňky vychází s AT příkazu +CREG. Kód buňky (Cell ID) je zde uveden jako část odpovědi po tomto příkazu. Přesněji parametr <ci>, který odpovídá posledním uvozovkám.

#### Příkaz týkající se úrovně signálů - AT+CSQ

Testovací příkaz: AT+CSQ=? Odpověď: výčet <rssi>, <ber>

Prováděcí příkaz: AT+CSQ Odpověď: <rssi>, <ber>

Parametry:	<rssi>	Přijímaný výkon
	0	-113 dBm nebo méně
	1	-111 dBm
	2-30	-109 až -53 dBm
	31	-51 dBm nebo více
	<ber>	Bitová chybovost
	0-7	Odpovídá RXQUAL viz literatura [ 6]
	99	Neznámá

SIEMENS C35i: AT+CSQ Odpověď: 18,99

SIEMENS C60: AT+CSQ Odpověď: 21,99

Za pomoci kódu primární buňky (Cell ID) a kódu lokace (LAC) viz výše (kapitola 2.5.2) lze pomoci neoficiálních seznamu základnových stanic (BTS) zjistit polohu této stanice. Neoficiální

seznamy stanic BTS pro většinu českých operátorů jsou uvedené na internetových stránkách „www.gsmweb.cz“ [ 13].

Hodnoty získané v této skupině se často mění proto je třeba je pravidelně aktualizovat.

#### 2.5.4 Skupina Sousední buňky

Tato skupina uvádí seznam sousedních buněk, sílu signálu, NCC, BCC a číslo kanálu, které jsou vysílány v BCCH a dekodovány podle norem [ 4], [ 5].

##### Příkaz SIM Toolkit

##### - AT^SSTK

Testovací příkaz: AT^SSTK=? Odpověď: <profile>

Nastavovací příkaz: AT^SSTK=<length>[, <mode>]<CR>PDU<ctrl-Z/ESC>

Odpověď: OK/ERROR/+CME ERROR

Parametry:	<length>	Délka PDU
	<mode>	0 Jeden příkaz
		1 Sekvence příkazu
	<pdu>	Příkazy SIM Toolkit viz GSM 11.14 [ 4]

Příkaz PDU [ 4], [ 5], [ 7]: „D009 8103012602 82028182“

D0 Proactive SIM command tag – značka směr ze SIM na MS

09 Length – délka (9 byte)

81 Command details tag – detaily značky

03 Length – délka (3 byte)

01 Command number – číslo příkazu

26 Command: provide local info – požadavek MS na informaci SIM

00 = Location Information – MCC, MNC, LAC a Cell ID

01 = IMEI telefonu

02 = Network Measurement results – výsledky měření sítě

03–FF = Reserved

82	Device identities tag
02	Length – délka (2 byte)
81	Source device identity – Zdroj (01 – Klávesnice, 02 – Display, 03 – Sluchátko, 81 – SIM, 82 – MS, 83 – Síť)
82	Source device identity – Cíl (01 – Klávesnice, 02 – Display, 03 – Sluchátko, 81 – SIM, 82 – MS, 83 – Síť)

Příkaz PDU načítá naměřená data sítě uložená na SIM do mobilní stanice (MS).

Odpověď od C60: „810301260282028281 830100 9610  
2626019C4DEA2044CD5A24A9029270BD 9D0D  
0741E080370E83B0F04B1406B0“

První skupina viz příkaz PDU pouze změna zdroje a cíle (Zdroj = 82 – MS, Cíl = 81 – SIM).

83	Result tag – Výsledná značka
01	Length – délka (1 byte)
00	Command performed successfully – příkaz proveden úspěšně
96	Network Measurement results tag – značka výsledků měření sítě
10	Length – délka (16 byte)

2	6	2	6	0	1	9	C	4	D	E	A	2	0	4	4
00100	01100	01001	01100	00000	00011	00111	000100	11011	11101	01000	100000	01000	0100	0100	0100
12	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
C	D	5	A	2	4	A	9	0	2	9	2	7	0	B	D
1100	1101	0101	1010	0010	0100	1010	1001	0000	0010	1001	0010	0111	0000	1011	1101
17	18	19	20	21	22	23	24	25	26	27	28				

Tabulka 2.3 Rozklad datové části PDU řetězce - sousední buňky

1	-	BA-USED (1 bit)	
2	-	DTX-USED (1 bit)	
3	-	RXLEV-FULL-SERVING-CELL -	100110 - 38
4	-	Spare (1 bit) – Oddělovací	

5	-	Measurement-Valid-Bit (1 bit) – Platné / neplatné			
6	-	RXLEV-SUB-SERVING-CELL	-	10 <b>0110</b>	38
7	-	Spare (1 bit) – Oddělovací			
8	-	RXQUAL-FULL-SERVING-CELL	-	000	0
9	-	RXQUAL-SUB-SERVING-CELL	-	<b>000</b>	0
10	-	NO-NCELL	-	<b>110</b>	6
11	-	RXLEV-NCELL 1	-	01 <b>1100</b>	28
12	-	BCCH-FREQ-NCELL 1	-	0100 <b>1</b>	9
13	-	BSIC-NCELL 1	-	<b>101</b> 111	5, 7
14	-	RXLEV-NCELL 2	-	0 <b>10100</b>	20
15	-	BCCH-FREQ-NCELL 2	-	010 <b>00</b>	8
16	-	BSIC-NCELL 2	-	<b>000</b> 100	0, 4
17	-	RXLEV-NCELL 3	-	<b>0100</b> 11	19
18	-	BCCH-FREQ-NCELL 3	-	00 <b>110</b>	6
19	-	BSIC-NCELL 3	-	<b>101</b> 01 <b>1</b>	5, 3
20	-	RXLEV-NCELL 4	-	<b>01000</b> 1	17
21	-	BCCH-FREQ-NCELL 4	-	<b>00100</b>	4
22	-	BSIC-NCELL 4	-	1010 <b>10</b>	5, 2
23	-	RXLEV-NCELL 5	-	<b>010000</b>	16
24	-	BCCH-FREQ-NCELL 5	-	<b>00101</b>	5
25	-	BSIC-NCELL 5	-	001 <b>001</b>	1, 1
26	-	RXLEV-NCELL 6	-	<b>001110</b>	14
27	-	BCCH-FREQ-NCELL 6	-	<b>00010</b>	2
28	-	BSIC-NCELL 6	-	<b>111</b> <b>101</b>	7, 5

9D BCCH channel list tag

0D Length – délka (13 byte)

0 7 4 1 E 0 8 0 3 7 0 E 8 3 B  
 0000**0111**0100**0001**11110**0000**1000**0000**0011**0111**0000**1110**1000**0011**1011  
                   |                  |                  |                  |                  |                  |  
                   1                  2                  3                  4                  5                  6

0 F 0 4 B 1 4 0 6 B 0  
 00001111**0000**0100**1011**0001**0100**0000**0110**1011**0000**  
                   |                  |                  |                  |  
                   7                  8                  9                  0

Tabulka 2.4 Rozklad datové části PDU řetězce – seznam kanálu

1	-	ARFCN – Absolute Radio Frequency Channel Number -	0000 <b>0111</b> 01	-	29
2	-	ARFCN – Absolute Radio Frequency Channel Number -	00 <b>0001</b> 1110	-	30
3	-	ARFCN – Absolute Radio Frequency Channel Number -	<b>0000</b> 1000 <b>00</b>	-	32
4	-	ARFCN – Absolute Radio Frequency Channel Number -	<b>00</b> 0011 <b>0111</b>	-	55
5	-	ARFCN – Absolute Radio Frequency Channel Number -	0000 <b>1110</b> 10	-	58
6	-	ARFCN – Absolute Radio Frequency Channel Number -	00 <b>0011</b> 1011	-	59
7	-	ARFCN – Absolute Radio Frequency Channel Number -	<b>0000</b> 1111 <b>00</b>	-	60
8	-	ARFCN – Absolute Radio Frequency Channel Number -	<b>00</b> 0100 <b>1011</b>	-	75
9	-	ARFCN – Absolute Radio Frequency Channel Number -	0001 <b>0100</b> 00	-	80
0	-	ARFCN – Absolute Radio Frequency Channel Number -	00 <b>0110</b> 1011	-	107

ARFCN odpovídá pořadovému číslu BCCH-FREQ-NCELL, kde nula je podle norem na posledním místě [ 6].

Hodnota RXLEV je vztažena k rozmezí 0 až 63. Převod mezi číslem a hodnotou je uveden níže [ 6].

RXLEV	0	=	méně než	-110 dBm.
RXLEV	1	=	-110 dBm	až -109 dBm.
			:	
			:	
RXLEV	62	=	-49 dBm	až -48 dBm.
RXLEV	63	=	vice než	-48 dBm.

Tabulka 2.5 Převodu číselných hodnot RXLEVEL na úroveň signálu

SIEMENS C60: AT^SSTK=11 Odpověď: > (čeká na PDU)

<pdu> D009810301260282028182(CTR+Z)

Odpověď

81030126028202828183010096102626019C4DEA2044CD5A24A902927

0BD9D0D0741E080370E83B0F04B1406B0

SIEMENS C35i: AT^SSTK=11 Odpověď: > (čeká na PDU)

<pdu> D009810301260282028182(CTR+Z)

Odpověď

81030126028202828183010096102020019E0D2910948C6A473114505

A4A9D100002E00032AA00000000C40000000000

*Interpretace pro SIEMENS C60:*

CellID	CH	RL	NB
<b>S</b>		-72	
<b>1</b>	080	-82	57
<b>2</b>	075	-90	04
<b>3</b>	059	-91	53
<b>4</b>	055	-93	52
<b>5</b>	058	-94	11
<del><b>6</b></del>	<del>030</del>	<del>-96</del>	<del>75</del>

*Tabulka 2.6 Seznam sousedních buněk C60 interpretace s BCCH*

*Interpretace pro SIEMENS C35i:*

CellID	CH	RL	NB
<b>S</b>		-78	
<b>1</b>	000	-80	51
<b>2</b>	000	-92	11
<b>3</b>	000	-92	15
<b>4</b>	784	-92	14
<b>5</b>	000	-93	11
<b>6</b>	000	-99	50

*Tabulka 2.7 Seznam sousedních buněk C35i interpretace s BCCH*

1, 4, 5, 6, 8, 9, 0 ARFCN = 000

2 ARFCN = 050; 3 ARFCN = 680; 7 ARFCN = 784

### 3. Aplikace pro monitorování parametrů v GSM

V kapitole 2 jsem provedl rozbor parametrů pro monitorování sítě GSM. Podkapitola 2.5 obsahuje popis příkazů, testy a způsob zpracování získaných parametrů. Tyto informace využívám při vytvoření mé aplikace.

Podle pokynu vedoucího, jsem vytvořil aplikaci, k monitorování parametrů v GSM síti druhé generace. Aplikace je tvořena v prostředí programovacího jazyka Delphi a odzkoušena na dvou mobilních telefonních přístrojích značky SIEMENS. Chování na jiných přístrojích je nutno odzkoušet popřípadě přizpůsobit danému výrobcí a typu. Dále se předpokládá pozdější využití v laboratorním cvičení, proto možná bude nutné některé funkce doplnit nebo upravit. Z tohoto důvodu je přiložen plný zdrojový kód.

#### 3.1 Hardwarové vybavení

Pro tuto diplomovou práci jsem použil mě dostupné dva mobilní přístroje značky SIEMENS C35i a C60. Každý přístroj jsem vybavil datovým kabelem a SIM kartou. V obou případech to byly datové kabely vybavené sériovým rozhraním. Nastavení pro jednotlivé telefony jsou uvedeny na internetových stránkách [ 14]. Možnost připojení přes USB kabely jsem pro tuto realizaci nepoužil. PC jsem využíval k programování aplikace. Notebook jsem používal k testu mnou vytvořené aplikace v terénu. Z PC mám přímo vyvedený sériový port, ale notebook tento port nemá. Proto bylo nutné pro něho zakoupit redukci USB - sériový port.

#### 3.2 Softwarové vybavení

Aplikaci jsem programoval [ 16], [ 17] v operačním systému Windows XP Professional a testování prováděl ve Windows XP Home. Jako vývojové prostředí bylo použito Delphi 7 Personal. Pro komunikaci se sériovým portem v Delphi 7, jsem použil komponentu Async32. Pro spuštění mé aplikace na jiném počítači je zapotřebí ActiveX knihovna obsažená v Delphi.

##### 3.2.1 TMS Async32

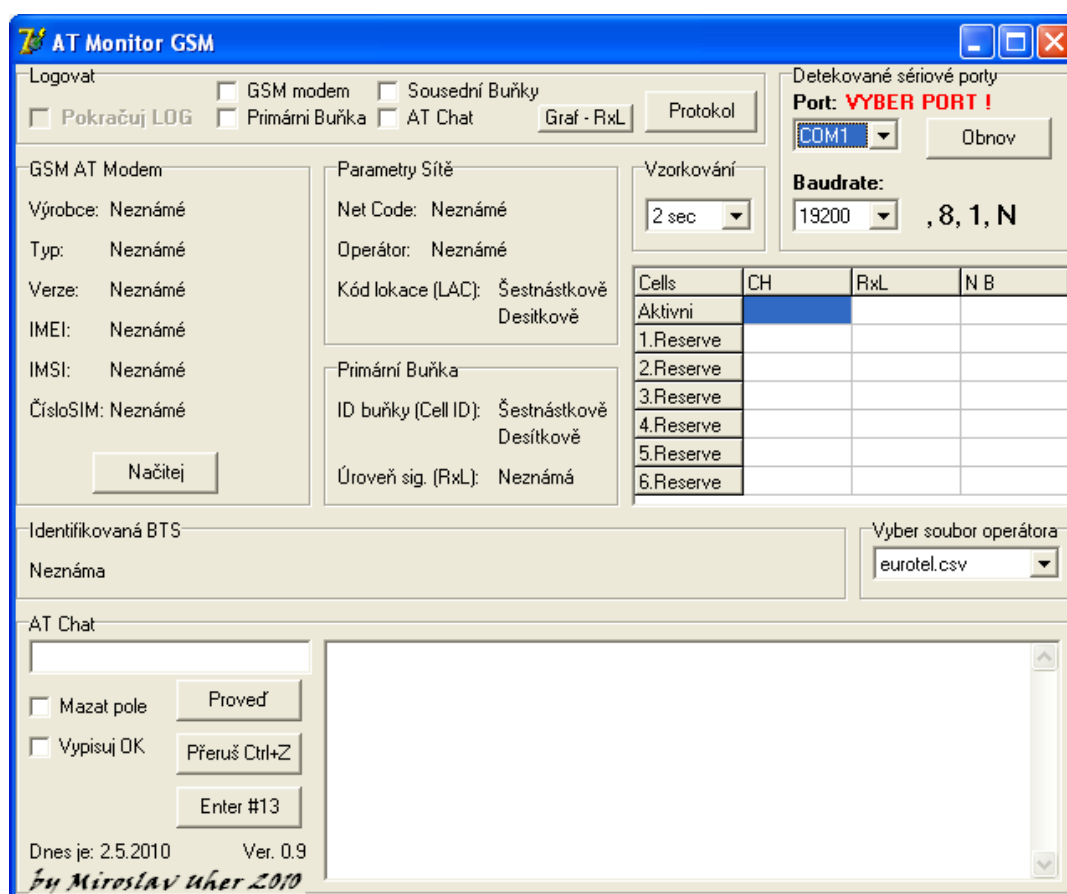
Balíček komponent společnosti TMS Software. TMS Async32 používám verzi 1.3.8.0 ze srpna 2008. Licence neumožňuje tento balíček komponentu šířit na přenosném médiu, proto ho nepřikládám ke zdrojovému kódu na CD (**Příloha 7**) určeném pro diplomovou práci, ale je ho třeba stáhnout z webových stránek výrobce „<http://www.tmssoftware.com/>“ [ 15].



### 3.3 Aplikace pro monitorování parametrů v GSM

#### 3.3.1 Aplikace AT Monitor GSM

Pro mou aplikaci jsem zvolil název „AT Monitor GSM“. Zkompilovaný program je zadán pod názvem „ATmonGSM.exe“. Její hlavní okno je uvedeno níže (viz *Obrázek 3.1*). Aplikace je tvořena jedním hlavním oknem, kde jsou ve skupinách uspořádané jednotlivé parametry, podle kritérií uvedených v kapitole 2.5 doplněny o funkce, které tyto parametry zpracovávají a ovládací prvky programu.



Obrázek 3.1 Aplikace AT Monitor GSM

#### 1. Skupiny zobrazující parametry:

GSM AT Modem  
Parametry Sítě  
Primární Buňka

#### 2. Skupiny s funkcí zpracování:

Sousední buňky (Cells)  
Identifikována BTS  
AT Chat

### 3. Skupiny nastavující:

Detekované sériové porty

Vyber soubor operátora

Vzorkování

Logovat

## 3.4 Tvorba aplikace AT Monitor GSM

Hlavní okno aplikace je výše (viz *Obrázek 3.1*). Jednotlivé skupiny uvedené v podkapitole 3.3.1, nyní rozeberu z pohledu tvorby a funkčnosti. Popis skupin následuje podle kroků tvorby programu. V kapitole 3.5 uvádím návrhy možných úprav a dalších funkcí, kterými by tato aplikace mohla být postupně doplňována. Text se odkazuje na zdrojový kód aplikace AT Monitor GSM přiložený v plném znění na CD (**Příloha 7**) k diplomové práci. Některé hlavní procedury uvádím v přílohách (viz **Příloha 1** až **Příloha 5**) a vysvětluji podrobněji.

### 3.4.1 Detekované sériové porty

Tato skupina je založena pro nastavení rozhraní přístupu k sériovému portu. Toto rozhraní je zprostředkováno balíkem komponent TMS Async32 [ 15]. V tomto případě využitím komponenty *VaComm*, která dokáže posílat a následně zachytávat textové řetězce na sériový port. Na této komponentě je postavená celá aplikace, nastavení se provádí v této skupině.

#### Ovládací prvky

Návěští „Port:“ informuje o stavu portu je vázáno na *ComboBox1*, kde se volí číslo portu. Po zvolení se změní nastavení komponenty *VaComm* viz kapitola 3.4.2 a port se otevře pro komunikaci (procedura *Vyber*). Návěští „Baudrate:“ odpovídá *ComboBox2*, lze nastavit komunikační rychlost sériového portu. Pokud byl port vybrán, procedura *Baudy* zavře port. Přenastaví se parametry rychlosti a znovu volá proceduru *Vyber*. Pokud byl program již spuštěn, je procedurou *Stop*, kvůli změnám parametru zastaven. Tato procedura je použita při každé změně. Text za výběrem informuje o dalším nastavení sériového portu a nelze měnit.

Tlačítko „Obnov“ provádí znovunačtení seznamu sériových portů z registrů Windows XP. Po stlačení je volána procedura *ObnovTL* pro změnu stylu výpisu, následně *Obnov* pro načtení seznamu. Program je zastavuje procedurou *Stop*.

### 3.4.2 Komponenta VaComm

Nastavení komponenty jsem provedl pro mou realizaci takto [ 18]:

- Parametr *AutoOpen* je vypnut (*False*). Je to otevření portu při zavedení komponenty. Pro mé účely je nutno nejdříve v aplikaci vybrat číslo portu.
- Parametr *Baudrate* je defaultně nastaven na 19200 Bd (*br19200*) z důvodu urychlení spouštění aplikace neboť většina mobilních přístrojů komunikuje touto rychlostí. V aplikaci lze tato hodnota měnit.
- Parametr *Databits* je nastaven na hodnotu 8 bitu (*db8*). Toto nastavení je stejné pro většinu MS, proto nelze v aplikaci změnit.
- Parametr *Stopbit* nastaven na 1 bit (*sb1*). Nelze v aplikaci také měnit.
- Parametr *PortNum* je pro vybrání čísla sériového portu. Nastavuje se až po vybrání z hlavní obrazovky.
- Skupinu parametrů *FlowControl* je třeba přednastavit:
  - Parametr *ControlDtr* což je pohotovost terminálu na hodnotu zapnuto (*dtrEnabled*).
  - Parametr *ControlRts* výzvu k vysílání na hodnotu zapnuto (*rtsEnabled*).

Ostatní parametry komponenty jsem ponechal výchozí. Reakce na události jsou volány v *Events* – *OnRxChar* což volá zachycení řetězce *CteniAT* a následně navazující zpracování *ATvypis*.

Pro načtení se používá jednoduchý příkaz komponenty, viz procedura níže:

```
procedure TForm1.CteniAT(Sender: TObject; Count: Integer);
                                //Čte vrácené hodnoty a dává je do at
begin
    at:=VaComm1.ReadText;      // Čtení textu z portu
    ATvypis;
                                // Posílá na COM po jednom AT příkazu
end;
```

kde proměna *at* obsahuje řetězec zachycený na sériovém portu a procedura *ATvypis* tento řetězec zpracuje. Po zpracování procedura zasílá přes sériový port další příkaz.

*Ovládání otevření a zavření portu je prováděno příkazy:*

```
VaComm1.Open;                                // Otevřít port
VaComm1.Close;                                // Zavření portu
```

*Změnu nastavení parametrů provedu například takto:*

```
VaComm1.PortNum:=port_c;                      // Změna portu podle proměnné
```

*Pro zápis na sériový port přes komponent se používá příkaz:*

```
VaComm1.WriteText('ATE1'+#13#10);
// Posílá na port příkaz - zapni echo
```

Při chybě otevření sériového portu volám proceduru `HandleException`.

### 3.4.3 AT Chat

Tato skupina byla vytvořená na počátku programování aplikace, pro potřeby návrhu a testy AT příkazů s komponentou *VaComm*. Nakonec jsem ji v aplikaci ponechal pro kontroly AT příkazů a ukázkou funkčnosti.

#### Ovládací prvky

Ve skupině je umístěn *Edit1* přes, který se zadávají příkazy (data) určené pro zpracování přes komponentu *VaComm* v AT modemu. Po stlačení tlačítka „Proved“ je obsah *Edit1* poslán na vybraný sériový port ukončený znaky #13#10 (enter, posuv vozíčku). Což je provedeno procedurou *Proved*, kde se také nastavují parametry (proměnné) zpracování *tlac=2* a *typ=1*. Určují nám při zachycení odpovědi v *CteniAT* a zavolání *ATvypis* část, která se provádí. Tlačítka „Přeruš Ctrl+Z“ a „Enter #13“ mají podobnou funkci jako uváděné výše, pouze s tím rozdílem, že znaky s *Edit1* jsou pro první tlačítko ukončeny znakem #26 a pro druhé #13. Při stisku tlačítek se běh aplikace zastaví a provádí se příkazy pouze ve skupině AT Chat.

Odpovědi, které posílá procedura `ATvypis` jsou vypisovány v poli `Memo1`. Ve formátu čas příkazu, zpracováváný příkaz. Na druhém řádku čas odpovědi, výsledná odpověď. Na odpověď je aplikována procedura `Znakym`, pro výmaz nadbytečných znaků.

Pro nastavení `Edit1`, je určen `ChackBox1` „Mazání pole“. Pokud je zaškrtnut, tak vymaže předešlý zadaný příkaz v editačním poli. Dalším nastavením je možnost výpisu potvrzení OK v odpovědi. Pro výpis je nutno zaškrtnout `ChackBox2` „Vypisuj OK“, čímž je vyřazeno s procedury `Znakym` mazání znaků, řetězec „OK“.

Informačně je zde uveden datum. Ve volném místě je nezávisle uvedena subjektivní verze aplikace a můj podpis pro identifikaci autor aplikace.

### 3.4.4 GSM AT Modem

Skupina sdružuje parametry identifikující modemu. Tyto hodnoty nejsou nijak zpracovány, jen načteny a po odstranění nadbytečných znaků vypsány.

### Ovládací prvky

Tlačítko „Načítej“ volá proceduru `Nacti` a AT příkazem pro zobrazování echa spouští provádění kódu. Parametry zpracování jsou nastaveny na `tlac=1`, `typ=1`. Při zachycení odpovědi v `CteniAT` se volá `ATvypis` s těmito parametry. Do jednotlivých `Label` jsou doplněné hodnoty. Prováděný program lze stejným tlačítkem jen s jiným popisem „Zastavit“ ukončit.

Po provedení načtení se aplikace sama nezastaví, ale je spuštěn `Timer`, který řídí další práci programu. Načítání parametrů sítě, primární buňky a další funkce, které jsou závislé na čase a potřebné pro zpracování zachytávaných odpovědí.

### 3.4.5 Parametry sítě

Načtení této skupiny je závislé na spuštění tlačítkem „Načítej“ a zapnutí `Timeru`. První výpis `Label` se provádí společně se skupinou GSM AT Modem. Další provedení výpisu je po 10 cyklech `Timeru`, z důvodu možnosti změny operátora. Pro časovou náročnost nastavení a zpracování v proceduře `KontrolaAT` a `ATvypis` této skupiny je `Timer` dočasně pozastaven a tím vzniká zpoždění ve výpisu cca 4 s. Pro opětovné zobrazení se spouští zpracovává `ATvypis`

s parametry `tlac=1`, `typ=6`. U *Label20* a *25* (LAC hex a dec) je výpis spouštěn při každém cyklu, kvůli návaznosti výsledné hodnoty na ID buňky (hex i dec) ve skupině primární buňky.

### 3.4.6 Primární Buňka

Načtení této skupiny je rovněž závislé na spuštění tlačítkem „Načítej“ a zapnutí *Timeru*. První výpis *Label* se provádí také se skupinou GSM AT Modem. Následně v každém cyklu *Timeru* se provede opětovné načtení parametru, přepočtení a zobrazení v *Label*. Zpracovává *ATvypis* je spuštěno s parametry `tlac=4`, `typ=1`. Hodnoty pro LAC a ID buňky, které jsou získané zároveň jedním AT příkazem, je třeba zpracovat procedurou *KontrolaP* a také převodem hexadecimálního čísla na dekadické, k čemu je určena procedura *Hexa*. Až pak je lze vypsat do příslušné *Label*. Pro zpracování hodnoty úrovně signálu do *Label* se volá procedura *KontrolaQ*.

Výsledné parametry načtené v této skupině jsou důležité pro nalezení a zobrazení dat ve skupině Identifikovaná BTS.

### 3.4.7 Vzorkování

Rychlost vzorkování se určuje v *ComboBox4* je v rozsahu 2 sekundy až 1 hodina. Při změně výběru volá *Vzorkovani* a tím nastaví rychlost *Timeru* na vybranou hodnotu. Změna také zastaví program. Rychlost vzorkování má vliv na chod celé aplikace a návaznost na většinu skupin.

### 3.4.8 Výběr souboru operátora

Při spuštění aplikace se do *ComboBox3* načtou názvy souboru s podadresáři „\Operatori“ s maskou `*.csv`, procedura *Vyhlop*. Načtené soubory se následně používají k vyhledání řádku s popisem BTS pro skupinu Identifikovaná BTS. Výběrem určíme startovací soubor operátora při prohledávání.

### 3.4.9 Identifikovaná BTS

Do tohoto pole se načítá popis BTS identifikovaný pomocí hodnot LAC a ID buňky, které označují řádek v souborech operátora „\*.csv“. Vyhledání a výpis se provádí v proceduře

Vyhledej, která je volána s `ATvypis`. Pokud nebyl ve vybraném souboru popis nalezen, je prohledávaný soubor automaticky změněn.

### 3.4.10 Sousední buňky

Vyplnění skupiny je závislé na spuštění tlačítka „Načítej“ a zapnutí *Timeru*. První naplnění *StringGrid1* je provedeno společně se skupinou GSM AT Modem. Každý cyklus *Timeru* hodnoty přepisuje, pokud je získán platný PDU řetězec (řetězec ukončený OK). Zpracovávání v `ATvypis` pokračuje ze skupiny Primární buňka s parametry `tlac=4`, `typ=1`, pouze pro interpretaci a zobrazení, je volána procedura `KontrolaBCCH` pro rozklad je použita procedura `Prevod`, která načítá řetězec po třech znacích.

### 3.4.11 Logovat

Skupina sdružuje *CheckBoxy*, které kontrolují, co se bude logovat. A které logovací soubory se budou vytvářet. Z této skupiny lze zobrazit také graf úrovně signálu.

### Ovládací prvky

Pro zaškrtnutí je *CheckBox3* zakázán, povolí se až při prvním spuštění aplikace z důvodu volání procedury `OznacChat` a podružných procedur `LogChat`, `LogModem`, `LogBTS` a `LogBCCH`. Při zaškrtnutí následujících čtyřech *Checkboxu* se vytvoří jednotlivé prázdné logovací soubory. Jejich umístění je v adresáři „\Log“. Masku přípony je „\*.log“. Při změně těchto ovládacích prvků se aplikace zastaví. *CheckBox3* umožňuje průběžné logování, to znamená, že nevytváří znovu prázdné logovací soubory při spuštění. Tlačítko „Protokol“ volá *Form3*, kde se nastaví hlavička protokolu a dalším tlačítkem lze spojit logovací soubory do jednoho protokolu. Tlačítko „Graf – RxL“ otvírá zobrazení grafu *Form2*, komponenta *VtChart*. Jsou zde dvě procedury. Jedna zobrazí a nastaví graf `FormShow`. Druhá doplňuje hodnoty do grafu `AddHodnoty`.

Jednotlivé řádky logovacích souborů se doplňují z procedury `ATvypis` voláním procedur `LogChatAdd`, `LogModemAdd`. Další procedury `LogBTSAdd` a `LogBCCHAdd`, které také dodávají řádky do logovacích souborů, jsou volány v proceduře `Casovac`.

### 3.4.12 Procedura ATvypis

Tuto procedu u uvádím v přílohách (viz **Příloha 1**). Ovládá větší část aplikace a provádí se hned po zachycení řetězce v `CteniAT`. Lze v ní vidět použití parametru spuštění `tlac` a `typ`. Následně jejich závislost na zpracovávání odpovědi příkazů a volání dalších příkazů, podle kapitoly 2.5. Důležitou částí této procedury je práce s řetězcí a to hlavně úpravy před zobrazení nebo pro další zpracování. Pro opakující se znaky je vytvořená procedura `Znaky`.

Pokud je zpracování řetězce složitější, volám na úpravu a výpis procedury. Například `KontrolaAT` nebo s jinými spouštěcími parametry procedury `KontrolaP`, `KontrolaQ` a `KontrolaBCCH`. Všechny tyto procedury kromě `KontrolaAT` se volají cyklicky podle časovače *Timer* a podmínek volání.

V tomto kódu je také vidět volání procedur pro zápis do logu `LogModemAdd`, `LogChatAdd` a za jakých podmínek probíhá.

### 3.4.13 Procedura KontrolaAT

Procedura `KontrolaAT` (viz **Příloha 2**) je spouštěna s `ATvypis` z části se spouštěcími parametry `tlac=1` a `typ=1`. Kde se vyhodnotí číslo země a operátora podle podkapitoly 2.5.2. Po zjištění typu odpovědi, se odstraní echo a nadbytečné znaky. Kontrolou typu odpovědi je ošetřeno různé chování rozdílných typů mobilních přístrojů.

Tato funkce je volána s `ATvypis` několikrát z důvodu nutnosti změny nastavení chování AT příkazu a opětovného vyhodnocení. Pro načtení čísla země a operátora při změně hodnot se volá po 10 cyklech *Timeru* opakovaně, pouze v `ATvypis` jsou použity spouštěcí parametry `tlac=1` a `typ=6`.

### 3.4.14 Procedura KontrolaP

Je uvedena na konci práce (viz **Příloha 3**). Zpracovává příkazy z kapitoly 2.5.3, kde se zjišťují parametry primární buňky. Je spouštěna s `ATvypis` z části se spouštěcími parametry `tlac=4` a `typ=1`. Po prvotní úpravě odstranění echa a nadbytečných znaků se volá na parametry procedura `Hexa`. Ta převádí získané hodnoty s hexadecimálních čísel na dekadická. Zpracování je ošetřeno podmínkami pro různé chování rozdílných typů mobilních přístrojů. Volání je prováděno periodicky podle rychlosti *Timeru* (Vzorkování).



### 3.4.15 Procedura KontrolaQ

Je spouštěna s `ATvypis` z části se spouštěcími parametry `tlac=4` a `typ=1`. Procedura je uvedena v přílohách (viz **Příloha 4**). Zjišťuje se v ní kvalita signálu podle popisu uvedeného v podkapitole 2.5.3. Po načtení odpovědi, se odstraní echo a nadbytečné znaky. Podle norem se pomocí podmínek následně zpracuje výsledek.

### 3.4.16 Procedura KontrolaBCCH

Procedura (**Příloha 5**) je spouštěna s `ATvypis` z části se spouštěcími parametry `tlac=4` a `typ=1`. Kde se dotazem načítá BCCH viz kapitoly 2.5.4. Po načtení odpovědi, se odstraní echo, PDU dotaz a nadbytečné znaky. Načte se určená pozice v řetězci pomocí procedury `Prevod` se převede do binární podoby a následně pomocí binárních posuvů vybere výsledná hodnota. První se zpracovává do pole seznam frekvenčních kanálů. Pak se zpracovává seznam sousedních buněk. Podle norem se pomocí podmínek a dalších funkcí zpracuje výsledek.

Další procedury neuvádím, neboť jsou komentované ve zdrojovém kódu a pro monitorování parametrů GSM sítě nejsou tak důležité jako tyto vybrané. Doplnují celek do funkční aplikace a zabezpečují správnou funkci jednotlivých procedur k zpracování AT příkazy. Popřípadě zabezpečují ovládání, logování, vykreslení grafu a vytvoření protokolu.

## 3.5 Možnosti rozšíření aplikace AT Monitor GSM

*Detekce sériového portu:*

- Vytvořit pro skupinu autodetekcí portu a nastavení.
- Rozšířit aplikaci o podporu USB kabelů.

*AT Chat:*

- Rozšířit volby o zobrazování povolení/zakázání echa.
- Možnost formátování zobrazení výstupních řetězců (mezery, enter, ctrl+z atd.).
- Nahrání a provedení skriptu s AT příkazy ze souboru.
- Zapnutí nezávislého časovače na opakování zadaného příkazu nebo na skript.

*GSM AT Modem, Parametry Sítě, Primární Buňka, Sousední buňky:*

- Oddělit zavolání příkazu od vyhodnocení. Vyhodnocovat nezávisle příchozí odpovědi, tím zkrátit možnost vzorkování na 1 s a odbourat nutnost vypínat průběh aplikaci při zápisu do AT Chatu nebo vyhodnocování odpovědi.
- Přizpůsobit zpracování i pro jiné značky mobilních přístrojů.
- Doplnit i o další parametry, které SIEMENS nemusí podporovat.
- Možnost znovu načtení defaultní konfigurace.

*Identifikovaná BTS:*

- Doplnit o možnost vynášení bodů přímo do internetové mapy.
- Možnost získání souřadnic.

*Vyber soubor operátora:*

- Doplnit o možnost aktualizace přímo z internetu.
- Identifikace, kdy byla poslední aktualizace provedena.
- Možnost doplnit i o soubory jiných operátorů.
- Možnost zvolit umístění složky se soubory operátorů.

*Logovat:*

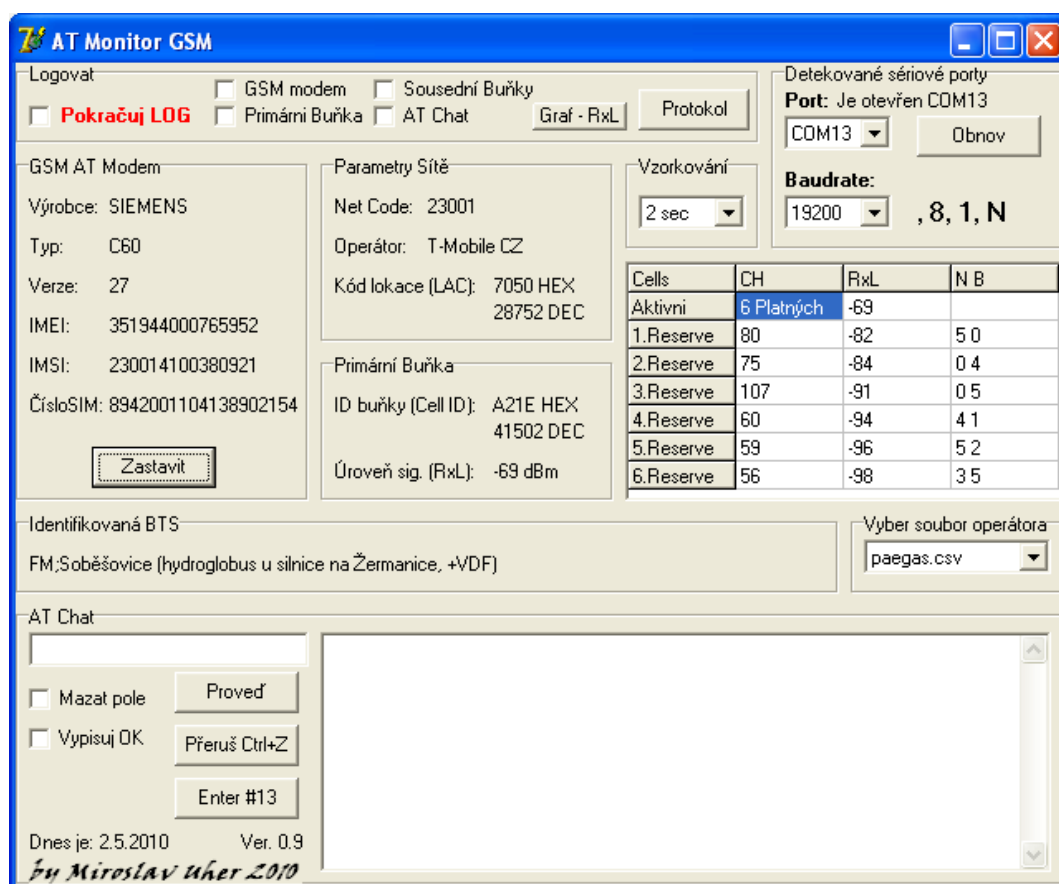
- Doplnit logování o soubor s nastavením programu při každé změně.
- Při logování GSM modemu zároveň s Parametry Sítě zapisovat pouze část, která se mění což je po deseti cyklech Parametry Sítě.
- Možnost změny umístění logovací složky.
- Rozlišení logovacích souborů (například pořadové číslo nebo datum vytvoření), zálohování.
- Při vytvoření protokolu nepřesouvat všechna data, ale jenom změny a tím odlehčit protokol.
- Graf je vytvořen pomocí komponenty *VtChart*, použít propracovanější komponentu.
- Doplnit do grafu zobrazení úrovně sousedních buněk.

## 4. Testování aplikace v reálných podmínkách

### 4.1 Zobrazení parametrů

Provedl jsem testování aplikace v reálných podmínkách. Na hlavní obrazovce (viz *Obrázek 4.1*) aplikace lze pozorovat parametry sítě podobně jako v servisním menu mobilního přístroje. Přehledně do skupin jsou zde seřazeny jednotlivé hodnoty parametru modemu, sítě, primární buňky a sousedních buněk.

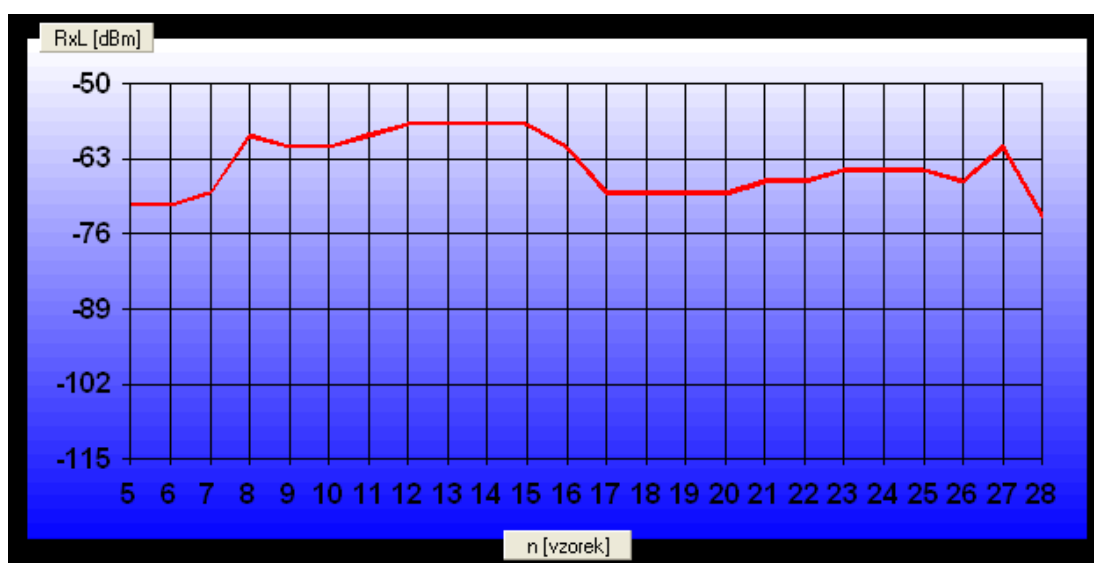
Načítání a zpracování se provádí v pravidelných časových intervalech podle hodnoty vzorkování. Změněny lze pozorovat přímo na hlavní obrazovce (*Obrázek 4.1*). Pokud tyto hodnoty namátkově srovnáme s obrazovkou servisního menu mobilního přístroje, tak zjistíme, že odpovídají. Proti reálným hodnotám je jejich výpis částečně zpožděn.



Obrázek 4.1 Test AT Monitor GSM v reálných podmínkách

### 4.1.1 Graf – Úrovně signálu

Pro lepší představu zobrazení příjmové úrovně signálu je možno v aplikaci zobrazit graf (viz *Obrázek 4.2*). V něm jsou vynášeny hodnoty úrovně signálu přijímané mobilním přístroji v závislosti na čase (vzorku času). Graf zároveň zobrazuje 24 vzorků úrovně. Jednotlivé vzorky jsou označeny pořadovým číslem. Začínají jedničkou při prvním zobrazení grafu.



Obrázek 4.2 Graf – Úroveň signálu

## 4.2 Logy

Další možností získání dat pro další zpracování je pomocí funkce logování. Při testu v reálných podmínkách je třeba v hlavním okně zaškrtnout potřebné logy, viz *Obrázek 4.1* skupina Logovat. Čímž průběžně zaznamenáváme hodnoty zobrazené v aplikaci a můžeme je později analyzovat.

### 4.2.1 GSM AT Modem a Parametry Sítě

Log zaznamenává hodnoty ve skupině GSM AT Modem a Parametry Sítě. Pravidelně je doplňován každých deset cyklu vzorkovacího času. Příklad prvního záznamu tohoto logovacího souboru je uveden na dalším listu (viz *Tabulka 4.1*).

```

AT Modem a parametry sítě logovací soubor
-----
Zachyceno: 29.4.2010 12:31:27
Výrobce: SIEMENS
Typ: C60
Verze: 27
IMEI: 351944000765952
IMSI: 230014100380921
ČísloSIM: 8942001104138902154
Net Code: 23001
Operátor: T-Mobile CZ
--

```

Tabulka 4.1 Logovací soubor Modem.log

#### 4.2.2 Primární Buňka

Další soubor loguje hodnoty a popis primární buňky. Sestavuje soubor z hodnot skupiny Primární Buňky a popisu uvedeného ve skupině Identifikovaná BTS. Záznamy se přidávají po jednom řádku za každý vzorek času. Několik záznamů ze souboru a hlavičku logu uvádím níže (viz Tabulka 4.2).

```

Identifikovaná BTS logovací soubor
-----
Zachyceno      Uroveň   LAC      CellID
Identifikovaná BTS
20.4.2010 10:43:44 -79 dBm  7050 HEX 28752 DEC  9FB2 HEX 40882 DEC
KI;Český Těšín - Koňákov, Hradištská (hydroglobus u silnice na Hradiště, +VDF)

20.4.2010 10:43:46 -73 dBm  7050 HEX 28752 DEC  A80B HEX 43019 DEC
KI;Český Těšín, náměstí Dr.Martina Luthera (evangelický kostel - schováno ve věži)

:
:

20.4.2010 10:43:56 -87 dBm  7050 HEX 28752 DEC  A80B HEX 43019 DEC
KI;Český Těšín, náměstí Dr.Martina Luthera (evangelický kostel - schováno ve věži)
..

20.4.2010 10:43:58 -87 dBm  7050 HEX 28752 DEC  A59F HEX 42399 DEC
KI;Český Těšín - Svibice, Kysucká 1824/12 (panelák na sídlišti Svibice)

```

Tabulka 4.2 Logovací soubor BTS.log

### 4.2.3 Sousední buňky

Pro sousední buňky je sestaven log z hodnot v tabulce Cells. Nový záznam je přidán na další řádek za každý vzorek času. Zachycený logovací soubor je uveden níže (viz *Tabulka 4.3*).

Datum	Buňka	Aktivni (RxL)	1.Buňka (CH RxL NB)	2.Buňka (CH RxL NB)
2.5.2010 15:39:07	6 Platných	-62	80 -78 5 0	75 -93 0 4
2.5.2010 15:39:12	6 Platných	-67	75 -79 0 4	75 -91 5 7
2.5.2010 15:39:17	6 Platných	-65	80 -78 5 0	75 -89 0 4
2.5.2010 15:39:22	6 Platných	-68	80 -78 5 0	75 -80 0 4
2.5.2010 15:39:27	6 Platných	-68	80 -80 5 0	56 -80 1 1
2.5.2010 15:39:32	6 Platných	-72	56 -83 1 1	75 -84 5 7
2.5.2010 15:39:37	6 Platných	-72	56 -80 1 1	75 -88 5 7

3.Buňka (CH RxL NB)	4.Buňka (CH RxL NB)	5.Buňka (CH RxL NB)	6.Buňka (CH RxL NB)
56 -80 1 1	59 -86 5 0	30 -94 5 7	107 -93 3 5
56 -81 1 1	59 -86 5 0	30 -94 5 7	32 -86 3 5
59 -82 5 3	55 -86 5 0	56 -87 2 2	30 -86 3 5
59 -84 5 3	56 -86 1 1	32 -87 6 1	55 -86 3 5
75 -81 0 4	107 -87 5 0	32 -94 6 1	30 -88 3 5
30 -89 7 4	107 -94 5 0	75 -94 0 1	32 -90 3 5
107 -91 7 4	59 -94 5 0	75 -94 0 1	32 -92 3 5

*Tabulka 4.3 Logovací soubor Sousedni.log*

### 4.2.4 AT Chat

Tento log zachytává AT příkazy a odpovědi vypisované na hlavní obrazovku. Nový záznam je přidán vždy po potvrzení zpracování. Příklad logovacího souboru je uveden hned pod textem (viz *Tabulka 4.4*).

```

AT Chat logovací soubor
-----
2.5.2010 16:55:08 P: AT+COPS?
2.5.2010 16:55:08 O: AT+COPS?+COPS: 0,2,"23001"
2.5.2010 16:55:26 P: AT+CREG?
2.5.2010 16:55:26 O: AT+CREG?+CREG: 0,1
2.5.2010 16:55:35 P: AT+CREG=2
2.5.2010 16:55:35 O: AT+CREG=2
2.5.2010 16:55:38 P: AT+CREG?
2.5.2010 16:55:38 O: AT+CREG?+CREG: 2,1,"7050","A21E"
2.5.2010 16:55:56 P: AT+CSQ
2.5.2010 16:55:56 O: AT+CSQ+CSQ: 21,99

```

*Tabulka 4.4 Logovací soubor Chat.log*

### 4.3 Protokol

Po dlouhodobém měření v reálných podmínkách jsou výstupem aplikace AT Monitor GSM logovací soubory. Jednotlivé příklady logu jsou uvedeny v kapitole 4.2. Po vytvoření protokolu se tyto jednotlivé soubory sloučí do jednoho hlavního souboru pojmenovaného Portokol.log s možností vyplnění hlavičky (Název protokolu, vypracoval).

K ověření činnosti v reálných podmínkách, jsem zvolil trasu Soběšovice – Frýdek-Místek. Doba zachytávání logovacích souborů byla cca 20 minut. Zachytávání bylo prováděno z jedoucího auta. V obci Dobrá byla dokonce zachycená neidentifikovaná BTS. Výstupní soubory jednotlivých logů a protokol, uvádím v příložené na CD (viz **Příloha 7**).

## 5. Závěr

V této diplomové práci jsem se zaměřil na monitorování parametrů v mobilních sítích druhé generace. Na začátku jsem provedl výběr parametrů, které lze v GSM sledovat. Po teoretickém rozboru jsem vybral z norem GSM příslušné AT příkazy a rovnou je prakticky testoval na mě dostupných mobilních telefonech značky SIEMENS. Odpovědi některých těchto příkazů bylo nutno ještě podle norem rozebrat a interpretovat. Tímto jsem měl teoretický základ pro tvorbu aplikace a pro monitorování těchto parametrů připraven.

Na počátku tvorby aplikace jsem zvolil připojení mobilního telefonu přes sériový port, protože jsem měl možnost získat takový datový kabel k telefonu značky SIEMENS, který mi byl doporučen k prvotním testům. Podle toho jsem volil i komponentu, která ovládá přístup k tomuto rozhraní v Delphi. Pokud by chtěl někdo tuto aplikaci využít i pro přístroje jiných značek je potřeba dodělat podporu USB. Pro většinu jiných mobilních přístrojů sériové datové kabely již nejsou dostupné. Hotovou aplikaci jsem neměl proto možnost na nich otestovat, případně pro ně upravit.

Aplikaci jsem programoval v programovacím prostředí Delphi. Dal jsem jí název „AT Monitor GSM“. K programování jsem využil vlastní zkušenosti a odkazy na mnohé internetové seriály k tomu programovacímu jazyku určené viz [ 18], [ 19], [ 20]. V některých částech jsem problém řešil jiným způsobem, než v předchozích. To proto, že jsem našel elegantnější programové řešení. Programovat jsem začal po malých blocích (skupinách), kdy jsem využíval teoretických podkladů uvedených na začátku práce v kapitole 2.5. Ověřuji funkci porovnáním výstupu aplikace s výsledky testovaných AT příkazů z kapitoly 2.5.

Při práci na aplikaci jsem začal řešit jednotlivé problémy a napadaly mě další možnosti vylepšení a rozšiřující funkce uvedl jsem je v kapitole 3.5. Aplikace je plně funkční a pro monitorování dostatečná, ale vývoj není ani zdaleka u konce. Tím že sdílím zdrojový kód, umožňuji další zpracování a možné úpravy například přizpůsobení pro laboratorní cvičení. Nyní je popis vztahen k aplikaci AT Monitor GSM v verzi 0.9.

Test aplikace v reálných podmínkách jsem provedl na trase Soběšovice – Frýdek-Místek. Aplikaci jsem měl spuštěnou na notebooku a nechal logovat parametry AT modemu, operátora, primární buňky a sousedních buněk po celou dobu jízdy. Zpracování do protokolu je uvedeno v kapitole 4.3.



## 6. Literatura

- [ 1 ] GSM 07.07 version 7.4.0 Release 1998. *Digital cellular telecommunications system (Phase 2+) : AT command set for GSM Mobile Equipment (ME)*. France : ETSI, 1999-11. 126 s. Dostupné z WWW: <<http://www.etsi.org>>.
- [ 2 ] GSM 07.05 version 5.5.0. *Digital cellular telecommunications system (Phase 2+); Use of Data Terminal Equipment - Data Circuit terminating : Equipment (DTE - DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS)*. France : ETSI, January 1998. 68 s. Dostupné z WWW: <<http://www.etsi.org>>. ISBN 2-7437-1945-1.
- [ 3 ] SIEMENS. *Manual Reference AT Command Set : (GSM 07.07, GSM 07.05, Siemens specific commands) for the SIEMENS Mobile Phones S35i, C35i, M35i*. [s.l.] : [s.n.], 15-03-2000. 52 s.
- [ 4 ] GSM 11.14 version 5.2.0. *Digital cellular telecommunications system (Phase 2+) : Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface*. France : ETSI, December 1996. 56 s. Dostupné z WWW: <<http://www.etsi.org>>. ISBN 2-7437-1205-8.
- [ 5 ] GSM 04.08 version 6.1.0 Release 1997. *Digital cellular telecommunications system (Phase 2+) : Mobile radio interface layer 3 specification*. France : ETSI, 1998-08. 593 s. Dostupné z WWW: <<http://www.etsi.org>>.
- [ 6 ] GSM 05.08 version 6.3.0 Release 1997. *Digital cellular telecommunications system (Phase 2+) : Radio subsystem link control*. France : ETSI, 1998-11. 57 s. Dostupné z WWW: <<http://www.etsi.org>>.
- [ 7 ] GSM-Forum [online]. 2003 [cit. 2010-05-03]. AT-commands for the Siemens networkmonitor?. Dostupné z WWW: <<http://forum.gsmhosting.com/vbb/f83/commands-siemens-networkmonitor-75839/>>.
- [ 8 ] HANUS, Stanislav. *Bezdrátové a mobilní komunikace*. Vyd. 1. V Brně : Vysoké učení technické, Fakulta elektrotechniky a informatiky, Ústav radioelektroniky, 2001. 134 s. ISBN 80-214-1833-8.
- [ 9 ] Subscriber Identity Module#Location area identity In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 5 January 2007, 3 May 2010 [cit. 2010-05-03]. Dostupné z WWW: <[http://en.wikipedia.org/wiki/Subscriber\\_Identity\\_Module#Location\\_area\\_identity](http://en.wikipedia.org/wiki/Subscriber_Identity_Module#Location_area_identity)>.

- 
- [ 10] C35i - legend by Gasbag [online]. 2001 [cit. 2010-05-03]. Dostupné z WWW: <<http://www.gasbag.wz.cz>>.
- [ 11] KOČMAN, Rostislav. *Servisní menu : Přehled známých popisů servisních menu mobilních telefonů*. Mobil.cz [online]. 6. listopadu 1999, , [cit. 2010-05-03]. Dostupný z WWW: <[http://mobil.idnes.cz/servisni-menu-0fg-/mob\\_tech.asp?c=A001106\\_0023924\\_mob\\_prakticky](http://mobil.idnes.cz/servisni-menu-0fg-/mob_tech.asp?c=A001106_0023924_mob_prakticky)>.
- [ 12] Lammert Bies - Computer Interfacing - Homepage [online]. c1997 [cit. 2010-05-03]. Hayes modem AT command set. Dostupné z WWW: <<http://www.lammertbies.nl/comm/info/hayes-at-commands.html>>.
- [ 13] MÁŠLO, Bronislav, et al. *GSMweb.cz* [online]. 1997-2010 [cit. 2010-05-03]. Dostupné z WWW: <<http://www.gsmweb.cz/>>.
- [ 14] STROLENÝ, Jaroslav. *DOVEDA BOYS - Procesory PIC12F629, PIC12F675, PIC16F84, PIC16F627, PIC16F628, PIC16F630, PIC16F676, PIC16F873, PIC16F874, PIC16F876 a PIC16F877* [online]. 1998-2010 [cit. 2010-05-03]. Srovnávací tabulky GSM telefonů. Dostupné z WWW: <<http://doveda.byl.cz/gsm/tabulka.htm>>.
- [ 15] TMS Software : *Productivity software building blocks* [online]. Verze 3.3. Nov 27, 2009 [cit. 2010-05-03]. TMS Async32. Dostupné z WWW: <<http://www.tmssoftware.com/site/async32.asp>>.
- [ 16] CANTÚ, Marco. *Mistrovství v Delphi 2 pro Windows 95/NT*. Praha : Computer Press, 1996. 975 s. ISBN 80-85896-75-3.
- [ 17] TEIXEIRA, Steve; PACHECO, Xavier. *Mistrovství v Delphi 6*. Vyd. 1. Brno : Computer Press, 2002. 822 s. ISBN 80-7226-627-6.
- [ 18] VYKOPAL, Jan. *Builder - Informační server o programování* [online]. 20.11. 2001 [cit. 2010-05-03]. Sériové rozhraní v Delphi. Dostupné z WWW: <<http://www.builder.cz/tiraz.php?uid=164>>.
- [ 19] ŠINDELÁŘ, Jan. *O počítačích, IT a internetu - Živě.cz* [online]. 25. 7. 2001 [cit. 2010-05-03]. Tipy a triky v Delphi. Dostupné z WWW: <<http://www.zive.cz/clanky/tipy-a-triky-v-delphi-dil-50---rekapitulace/sc-3-a-107738/default.aspx>>.
- [ 20] KADLEC, Václav. *O počítačích, IT a internetu - Živě.cz* [online]. 19. 3. 2001 [cit. 2010-05-03]. Umíme to s Delphi. Dostupné z WWW: <<http://www.zive.cz/clanky/umime-to-s-delphi--1-dil/sc-3-a-30959/default.aspx>>.

## **PŘÍLOHY**

**Příloha 1:** Procedura ATvypis

**Příloha 2:** Procedura KontrolaAT

**Příloha 3:** Procedura KontrolaP

**Příloha 4:** Procedura KontrolaQ

**Příloha 5:** Procedura KontrolaBCCH

**Příloha 6:** Návod k aplikaci AT Monitor GSM

**Příloha 7:** Datový nosič - CD

**Příloha 1: Procedura ATvypis**

```
procedure TForm1.ATvypis;           // Zabezpečuje výpis a návrat po AT příkazu
var
  Uroven: String;                   // Popis úrovně pro graf

begin
case tlac of                         // Zmačknute tlačítko
1:begin
  case typ of                         // Číslo příkazu
  1:begin
    VaComm1.WriteText('AT+CGMI'+#13#10); // Dotaz na výrobce AT příkazem
  end;
  2:begin
    at:=StringReplace(at, 'ATE1', '', [rfReplaceAll]); // Nahradí znaky kvůli chybě

    atm:=StringReplace(at, 'AT+CGMI', '', [rfReplaceAll]); // Nahradí znaky echa
    Znakym;           // Smazání znaku
    Label3.Caption:=atm; // Výrobce

    VaComm1.WriteText('AT+CGMM'+#13#10); // Dotaz na typ AT příkazem
  end;
  3:begin
    atm:=StringReplace(at, 'AT+CGMM', '', [rfReplaceAll]); // Nahradí znaky echa
    Znakym;           // Smazání znaku
    Label4.Caption:=atm; // Typ

    VaComm1.WriteText('AT+CGMR'+#13#10); // Dotaz na verzi AT příkazem
  end;
  4:begin
    atm:=StringReplace(at, 'AT+CGMR', '', [rfReplaceAll]); // Nahradí znaky echa
    Znakym;           // Smazání znaku
    Label5.Caption:=atm; // Verze

    VaComm1.WriteText('AT+CGSN'+#13#10); // Dotaz na IMEI AT příkazem
  end;
  5:begin
    atm:=StringReplace(at, 'AT+CGSN', '', [rfReplaceAll]); // Nahradí znaky echa
    Znakym;           // Smazání znaku
    Label6.Caption:=atm; // IMEI

    VaComm1.WriteText('AT+CIMI'+#13#10); // Dotaz na IMSI AT příkazem
  end;
  6:begin
    if opakuj=0 then                 // Kvůli zkrácení opakování
    begin
      atm:=StringReplace(at, 'AT+CIMI', '', [rfReplaceAll]); // Nahradí znaky echa
      Znakym;           // Smazání znaku
      Label13.Caption:=atm; // IMSI
    end;

    VaComm1.WriteText('AT+COPS=3,0'+#13#10); // Nastavení formátu výpisu operátora
  end;
  7:begin
    VaComm1.WriteText('AT+COPS?'+#13#10); // Dotaz na operátora AT příkazem
  end;
  8:begin
    KontrolAT;
```

```

        VaComm1.WriteText('AT+COPS=3,2'+#13#10); // Dotaz na operátora změněný formátu
    end;
9:begin
    VaComm1.WriteText('AT+COPS?'+#13#10); // Dotaz na operátora AT příkazem
end;
10:begin
    KontrolaT;

    VaComm1.WriteText('AT^SCID'+#13#10); // Dotaz na číslo SIM AT příkazem
end;
11:begin
    atm:=StringReplace(at, 'AT^SCID', '', [rfReplaceAll]); // Nahradí znaky
    atm:=StringReplace(atm, '^SCID: ', '', [rfReplaceAll]); // Nahradí znaky
    Znakym; // Smazání znaku

    Label17.Caption:=atm; // Číslo SIM

    Button2.Caption:='Zastavit'; // Přepisuje jméno B2
end;
end;
Inc(typ); // Posouvá na další příkaz
Sleep(cekani); // Čas na zpracování v mobilu

if typ=12 then // POZOR 12 kontrola poslední položky
begin
    if CheckBox4.Checked=True then LogModemAdd; // Dodá řádek do LogModem -Pouze jednou
    Timer1.Enabled:=True; // Spouští timer
end;
end;

2:begin // Chat část
    case typ of
    { 1:begin
        VaComm1.WriteText(Edit1.Text+#13#10);
        end; }
    1:begin
        atm:=at; // Kvůli změně na výstupu
        at:=''; // Vynulovat at
        Memo1.Lines.Add(TimeToStr(Time)+' P: '+Edit1.Text); // Čte data z Edit
        Znakym; // Smaže nadbytečné znaky
        Memo1.Lines.Add(TimeToStr(Time)+' O: '+atm); // Čte portu zápis do Mema
        if CheckBox6.Checked=True then LogChatAdd; // Dodá řádek do LogChat
        if CheckBox1.Checked=True then Edit1.Clear; // Maže editbox - Check1
        end;
    end;
    Inc(typ); // Posouvá na další příkaz
    Sleep(cekani); // Čas na zpracování v mobilu
end;

4:begin // Po zapnutí timeru proměna část
    case typ of
    1:begin
        VaComm1.WriteText('AT+CREG=0'+#13#10); // Představit na at+creg=0
        end;
    2:begin
        VaComm1.WriteText('AT+CREG?'+#13#10); // Načtení CellID a LAC
        end;
    3:begin

```

---

```
KontrolP;                                // Kontrola AT
VaComm1.WriteText('AT+CREG=2'+#13#10);    // Představit na at+creg=2
end;
4:begin
    VaComm1.WriteText('AT+CREG?'+#13#10);    // Načtení CellID a LAC
end;
5:begin
    KontrolP;                                // Kontrola AT
    VaComm1.WriteText('AT+CREG=0'+#13#10);    // Představit na at+creg=0
    Vyhledej;                                // Vyhledá BTS
end;
6:begin
    VaComm1.WriteText('AT+CSQ'+#13#10);        // Úroveň signálu
end;
7:begin
    KontrolQ;                                // Kontrola kvality

    Uroven:=Label24.Caption;                    // Načte hodnotu úrovně
    Uroven:=StringReplace(Uroven, ' dBm', '', [rfReplaceAll]); // Ubrat jednotky

    if Form2.Visible then Form2.AddHodnota(Uroven); // Spouští se pořad ošetření
    VaComm1.WriteText('AT^SSTK=11,0'+#13);        // Dotaz na sousední buňky
end;
8:begin
    VaComm1.WriteText('D009810301260282028182'+#26#13); // Dotaz
end;
9:begin
    KontrolaBCCH;
end;

end;
Inc(typ);                                // Posouvá na další příkaz
Sleep(cekani);                            // Čas na zpracování v mobilu
end;
end;
```

**Příloha 2: Procedura KontrolaAT**

```
procedure TForm1.KontrolaAT;                                // Výpis do Label podle typu
begin
    atm:=at;
    at:='';

    if (pos('+COPS: 0,2','',atm)>0) then                    // Smaž podle typu - do jedné podmínky
    begin
        atm:=StringReplace(atm, 'AT+COPS?', '', [rfReplaceAll]); // Odstranění příkazu: echo
        Delete(atm,Pos('+COPS: 0,2','',atm),12);           // Odstranění znaků +COPS: 0,2
        atm:=StringReplace(atm, '','', '', [rfReplaceAll]); // Odstranění uvozovek
        Znakym;                                             // Smazání znaku

        Label16.Caption:=atm;                               // Net code
        exit;
    end;

    // if ((pos('AT+COPS?',atm)>0) and
    if(pos('+COPS: 0,0','',atm)>0) then
    begin
        atm:=StringReplace(atm, 'AT+COPS?', '', [rfReplaceAll]); // Odstranění příkazu: echo
        Delete(atm,Pos('+COPS: 0,0','',atm),12);           // Odstranění znaků +COPS: 0,0
        atm:=StringReplace(atm, '','', '', [rfReplaceAll]); // Odstranění uvozovek
        Znakym;                                             // Smazání znaku

        Label18.Caption:=atm;                               // Operátora
        exit;
    end;
end;
```

**Příloha 3: Procedura KontrolaP**

```

procedure TForm1.KontrolaP;                                // Výpis do Label podle typu
begin
    atm:=at;                                                // Kvůli změně na výstupů
    at:='';                                                // Vynulování at

    if (pos('AT+CREG?',atm))>0 then                        // Chyba opakování
    begin
        Znakym;                                            // Smazání nadbytečných znaků
        Delete(atm,Pos('AT+CREG?',atm),8);                // Odstranění znaků +CREG?
        hxdc:=atm;
        if (Pos('+CREG: 0,1','',hxdc))>0 then Delete(hxdc,Pos('+CREG: 0,1','',hxdc),12) else
            // Odstranění znaků +CREG: 0,1, z čísla LAC
            if (Pos('+CREG: 2,1','',hxdc))>0 then Delete(hxdc,Pos('+CREG: 2,1','',hxdc),12) else
exit;                                                    // Odstranění znaků +CREG: 2,1, z čísla LAC

        Delete(hxdc,Pos('','',hxdc),10);                  // Odstranění znaků " z čísla LAC
        Label20.Caption:=hxdc+' HEX';                     // LAC v šestnáctkové soustavě

        if hxdc[1]='+' then else                          // Musí se ošetřit jiný VYSLEDEK
        begin
            Hexa;                                          // Převod
            LacVy:=hxdc;
        end;
        Label25.Caption:=hxdc+' DEC';                     // LAC převedený na Dec
        hxdc:=atm;
        if (Pos('+CREG: 0,1','',hxdc))>0 then Delete(hxdc,Pos('+CREG: 0,1','',hxdc),19) else
            if (Pos('+CREG: 2,1','',hxdc))>0 then Delete(hxdc,Pos('+CREG: 2,1','',hxdc),19) else
exit;

        Delete(hxdc,Pos('','',hxdc),3);                  // Odstranění znaků " z čísla ID Cell
        Label22.Caption:=hxdc+' HEX';                     // ID Cell v šestnáctkové soustavě
        if hxdc[1]='+' then else                          // Musí se ošetřit jiný VYSLEDEK
        begin
            Hexa;                                          // Převod
            CidVy:=hxdc;
        end;
        Label26.Caption:=hxdc+' DEC';                     // ID Cell převedený na Dec
    end;
end;

```



**Příloha 4: Procedura KontrolaQ**

```
procedure TForm1.KontrolaQ;                                // Kontrola kvality signálu
begin
    atm:=at;                                                // Kvůli změně na výstupu
    at:='';                                                // Vynuluje at

    Znakym;                                                // Smaže nadbytečné znaky
    atm:=StringReplace(atm, 'AT+CSQ', '', [rfReplaceAll]); // Odstranění příkazu echo
    atm:=StringReplace(atm, '+CSQ: ', '', [rfReplaceAll]); // Odstranění znaků +CSQ:
    Delete(atm, Pos(' ', atm), 5);                         // Odstranění znaků "

    if atm=IntToStr(0) then
    begin
        Label24.Caption:='-113'+ ' dBm';                  // Výpis dle normy
        exit;
    end;

    if atm=IntToStr(1) then
    begin
        Label24.Caption:='-111'+ ' dBm';
        exit;
    end;

    if atm>IntToStr(1) then
    begin
        if atm<IntToStr(31) then
        begin
            Label24.Caption:=IntToStr(((StrToInt(atm)-2)*2)-109)+' dBm';
            exit;
        end;

        if atm=IntToStr(31) then
        begin
            Label24.Caption:='-51'+ ' dBm';
            exit;
        end;

        if atm=IntToStr(99) then Label24.Caption:='Neznámá';
    end;
end;
```

**Příloha 5: Procedura KontrolaBCCH**

```

procedure TForm1.KontrolaBCCH;                                // Zkontroluje a rozloží BCCH
var
  p: integer;
  ch: array [0..15] of integer;                               // Pro načtení hodnot kanálů
  n: byte;

begin
  for p:=0 to 15 do ch[p]:=0;                                  // Inicializace pole
  if (Pos('8103012602820282818301009610',at)>0) and (Pos('OK',at)>0) then
  begin
    atm:=at;

    atm:=StringReplace(atm, 'D009810301260282028182', '', [rfReplaceAll]);
    atm:=StringReplace(atm, '^SSTK: ', '', [rfReplaceAll]);
    atm:=StringReplace(atm, '8103012602820282818301009610', '', [rfReplaceAll]);
    atm:=StringReplace(atm, '#26', '', [rfReplaceAll]);

    Znakym;

    poz:=37;                                                    // Zjištění vysílacích kanálu
    Prevod;                                                    // ARFCN 1
    mala:=mala shr 2;                                           // Načtení 2 bytu z pozice v PDU
    ch[1]:=velka*64+mala;                                       // Bitový posuv - ořezání bytu

    poz:=39;                                                    // ARFCN 2
    Prevod;
    velka:=velka shl 6;                                         // Bitový posuv - ořezání bytu
    velka:=velka shr 6;
    ch[2]:=velka*256+mala;

    poz:=42;                                                    // ARFCN 3
    Prevod;                                                    // Začíná se opakovat
    mala:=mala shr 2;                                           // Bitový posuv - ořezání bytu
    ch[3]:=velka*64+mala;

    poz:=44;                                                    // ARFCN 4
    Prevod;
    velka:=velka shl 6;                                         // Bitový posuv - ořezání bytu
    velka:=velka shr 6;
    ch[4]:=velka*256+mala;

    poz:=47;                                                    // ARFCN 5
    Prevod;                                                    // Začíná se opakovat
    mala:=mala shr 2;                                           // Bitový posuv - ořezání bytu
    ch[5]:=velka*64+mala;

    poz:=49;                                                    // ARFCN 6
    Prevod;
    velka:=velka shl 6;                                         // Bitový posuv - ořezání bytu
    velka:=velka shr 6;
    ch[6]:=velka*256+mala;

    poz:=52;                                                    // ARFCN 7
    Prevod;                                                    // Začíná se opakovat
    mala:=mala shr 2;                                           // Bitový posuv - ořezání bytu
    ch[7]:=velka*64+mala;
    poz:=54;                                                    // ARFCN 8

```

```
Prevod;
velka:=velka shl 6;           // Bitový posuv - ořezání bytu
velka:=velka shr 6;
ch[8]:=velka*256+mala;

poz:=57;                      // ARFCN 9                      // Začíná se opakovat
Prevod;
mala:=mala shr 2;             // Bitový posuv - ořezání bytu
ch[9]:=velka*64+mala;

poz:=59;                      // ARFCN 10
Prevod;
velka:=velka shl 6;           // Bitový posuv - ořezání bytu
velka:=velka shr 6;
ch[0]:=velka*256+mala;

poz:=1;                      // Rx1 S
Prevod;
mala:=mala shr 4;             // Bitový posuv - ořezání bytu
velka:=velka shl 6;
velka:=velka shr 6;
StringGrid1.Cells[2,1]:=IntToStr(-110+(velka*16+mala));

poz:=6;                      // Rx1 1
Prevod;
mala:=mala shl 2;             // Bitový posuv - ořezání bytu
mala:=mala shr 2;
velka:=0;
StringGrid1.Cells[2,2]:=IntToStr(-110+(mala));

poz:=11;                      // Rx1 2
Prevod;
mala:=mala shr 3;             // Bitový posuv - ořezání bytu
velka:=velka shl 7;
velka:=velka shr 7;
StringGrid1.Cells[2,3]:=IntToStr(-110+(velka*16+mala));

poz:=15;                      // Rx1 3
Prevod;
mala:=mala shr 2;             // Bitový posuv - ořezání bytu
velka:=0;
StringGrid1.Cells[2,4]:=IntToStr(-110+(mala));

poz:=19;                      // Rx1 4
Prevod;
mala:=mala shl 1;             // Bitový posuv - ořezání bytu
mala:=mala shr 2;
velka:=0;
StringGrid1.Cells[2,5]:=IntToStr(-110+(mala));

poz:=23;                      // Rx1 5
Prevod;
mala:=mala shl 2;             // Bitový posuv - ořezání bytu
mala:=mala shr 2;
velka:=0;
StringGrid1.Cells[2,6]:=IntToStr(-110+(mala));

poz:=28;                      // Rx1 6
Prevod;
```

```
mala:=mala shr 3;           // Bitový posuv - ořezání bytu
velka:=velka shl 7;
velka:=velka shr 7;
StringGrid1.Cells[2,7]:=IntToStr(-110+(mala));

poz:=8;                     // Ch 1
Prevod;
mala:=mala shr 3;           // Bitový posuv - ořezání bytu
velka:=0;
StringGrid1.Cells[1,2]:=IntToStr(ch[mala]);

poz:=12;                    // Ch 2
Prevod;
mala:=mala shl 1;           // Bitový posuv - ořezání bytu
mala:=mala shr 3;
velka:=0; StringGrid1.Cells[1,3]:=IntToStr(ch[mala]);

poz:=16;                    // Ch 3
Prevod;
mala:=mala shl 2;           // Bitový posuv - ořezání bytu
mala:=mala shr 3;
velka:=0; StringGrid1.Cells[1,4]:=IntToStr(ch[mala]);

poz:=20;                    // Ch 4
Prevod;
mala:=mala shl 3;           // Bitový posuv - ořezání bytu
mala:=mala shr 3;
velka:=0; StringGrid1.Cells[1,5]:=IntToStr(ch[mala]);

poz:=25;                    // Ch 5
Prevod;
mala:=mala shr 3;           // Bitový posuv - ořezání bytu
velka:=0;
StringGrid1.Cells[1,6]:=IntToStr(ch[mala]);

poz:=29;                    // Ch 6
Prevod;
mala:=mala shl 1;           // Bitový posuv - ořezání bytu
mala:=mala shr 3;
velka:=0; StringGrid1.Cells[1,7]:=IntToStr(ch[mala]);

poz:=9;                     // NB 1
Prevod;
n:=mala;

n:=n shl 4;
n:=n shr 5;

mala:=mala shl 1;           // Bitový posuv - ořezání bytu
mala:=mala shr 5;
velka:=0;
StringGrid1.Cells[3,2]:=IntToStr(mala)+' '+IntToStr(n);

poz:=13;                    // NB 2
Prevod;
n:=mala;                     // 00xx xxxx
```

```
n:=n shl 5;
n:=n shr 5;

mala:=mala shl 2;           // Bitový posuv - ořezání bytu
mala:=mala shr 5;
velka:=0;
StringGrid1.Cells[3,3]:=IntToStr(mala)+' '+IntToStr(n);

poz:=18;                    // NB 3
Prevod;
n:=mala;

n:=n shl 2;                 // nižší      x xxxx x000
n:=n shr 5;

mala:=mala shr 6;          // vyšší
velka:=velka shl 7;        // Bitový posuv - ořezání bytu
velka:=velka shr 7;
StringGrid1.Cells[3,4]:=IntToStr(velka*4+mala)+' '+IntToStr(n);

poz:=22;                    // NB 4
Prevod;
n:=mala;

n:=n shl 3;                // nižší      XXXX XX00
n:=n shr 5;

mala:=mala shr 5;          // vyšší
velka:=0;
StringGrid1.Cells[3,5]:=IntToStr(mala)+' '+IntToStr(n);

poz:=26;                    // NB 5
Prevod;
n:=mala;

n:=n shl 2;                // nižší      x xxxx x000
n:=n shr 5;

mala:=mala shr 6;          // vyšší
velka:=velka shl 7;
velka:=velka shr 7;
StringGrid1.Cells[3,6]:=IntToStr(velka*4+mala)+' '+IntToStr(n);

poz:=32;                    // NB 6
Prevod;
n:=mala;

n:=n shl 5;                // nižší      00xx xxxx
n:=n shr 5;

mala:=mala shl 2;          // vyšší
mala:=mala shr 5;
velka:=0;
StringGrid1.Cells[3,7]:=IntToStr(mala)+' '+IntToStr(n);
poz:=5;                    // Neplatné buňky      000x xx00
Prevod;
mala:=mala shl 3;          // Bitový posuv - ořezání bytu
mala:=mala shr 5;
```

```
    velka:=0;  
    StringGrid1.Cells[1,1]:=IntToStr(mala)+' Platných';  
  
    end;  
    // else atm:='špatně'; // necelý řetězec PDU  
    if CheckBox7.Checked=True then LogSousednichAdd; // Kontrola na zapis logu  
end;
```

**Příloha 6: Návod k aplikaci AT Monitor GSM**

# Návod k obsluze aplikace

## AT Monitor GSM

Verze 0.9

### Úvod

Tento dokument má sloužit jako návod k aplikaci AT Monitor GSM. Tato aplikace je určena pro monitorování parametrů mobilních sítí druhé generace za použití externího mobilního přístroje připojeného pomocí datového kabelu na sériový port. Byla naprogramována jako součást diplomové práce. Teorie k návodu je uvedena v této diplomové práci.

### Hardwarové a softwarové nároky

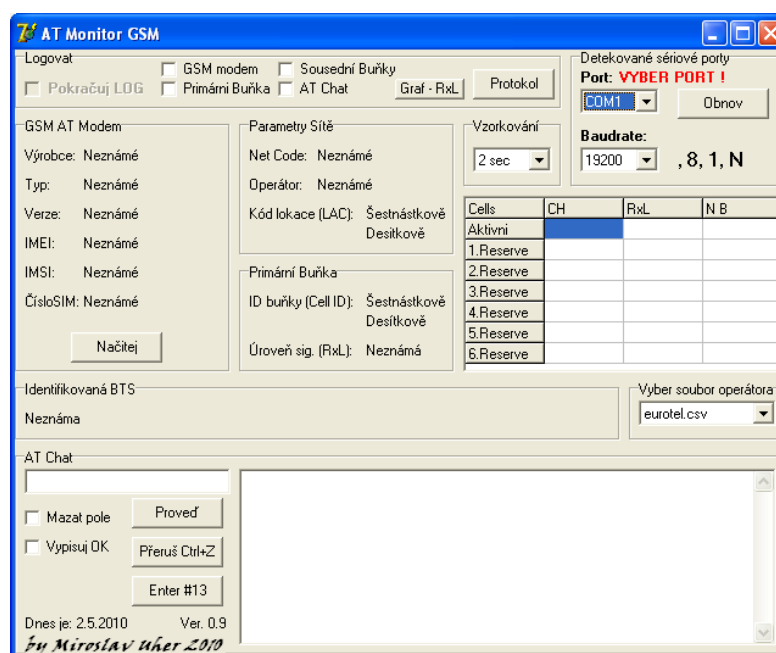
Aplikaci lze spustit na jakémkoliv stolním PC nebo notebooku, kde je nainstalován systém Windows XP. Pod jiným systémem aplikace nebyla zkoušena a proto může vyvolat chybu systému nebo nelze spustit. PC nebo notebook musí být vybaven alespoň jedním sériovým portem. Pokud tomu tak není je nutno ho dovybavit USB adaptérem sériového portu. Aplikace byla odzkoušena na mobilních přístrojích značky SIEMENS vybavených datovým sériovým kabelem.

K spuštění aplikace a správné funkci je třeba zaregistrovat ActiveX knihovnu pro zobrazení grafu.

*Postup registrace:* Soubory přiložené k programu v adresáři \Insatll\_ATmonGSM je třeba přkopírovat do systémové složky \Windows\system32 a následně zaregistrovat knihovnu příkazem - `regsvr32.exe vcfi32.ocx`.

## AT Monitor GSM

Po spuštění této aplikace se zobrazí hlavní okno, viz *Obrázek 1*. Z tohoto okna lze ovládat většinu funkcí programu.



*Obrázek 1 Test AT Monitor GSM v reálných podmínkách*

## Nastavení před spuštěním

Před spuštěním je možno nastavit několik parametrů ovlivňujících chování této aplikace při spuštění. Pokud budou změny provedeny v průběhu chodu aplikace, provádění se pozastaví. Aplikace pak musí být znovu spuštěna. Skupiny jsou členěny podle *Obrázku 1*.

### **Skupina Detekované sériové porty**

Obsahuje ovládací prvky potřebné k nastavení sériového portu a komunikace přes datový kabel.

*Výběr sériového portu* – seznam portů je uveden v rozbalovacím seznamu s označením „COM1“. Port je nutno vybrat, jinak nelze aplikaci spustit. Pokud v seznamu není uvedený port, je nutno použít tlačítko „Obnov“. Vybraný port je indikován v návěští „Port:“.

*Obnovení výčtu portu* – tlačítko „Obnov“ znovu načítá seznam portů do rozbalovacího seznamu.



*Výběr znakové rychlosti portu* – výpis rychlostí je uveden v rozbalovacím seznamu pod označením „**Baudrate:**“. Defaultně je vybrána hodnota 19200 Bd. Rychlost nastavujeme podle potřeb mobilního přístroje.

### **Skupina Vyber soubor operátor**

*Vyber soubor operátora* – v rozbalovacím seznamu je načten seznam souborů operátorů s příponou csv. Načítají se z adresáře programu, podadresář \Operatori. Pokud nebyl soubor vybrán, použije se defaultně zobrazený. Když v něm nebude identifikována BTS, soubor se automaticky změní (procházejí se všechny soubory v adresáři).

Aktualizované soubory lze získat na internetových stránkách „<http://www.gsmweb.cz/>“. Obsahují neoficiální seznamy umístění BTS.

### **Skupina Vzorkování**

*Výběr času vzorkování* – z rozbalovacího seznamu lze vybrat čas jednoho vzorku. Tento čas následně řídí intervaly, ve kterých se načítají hodnoty parametrů sítě.

Při změně je aplikace pozastavena.

### **Skupina Logování**

Obsahuje zaškrťovací tlačítka pro ovládání logování aplikace. Dále zde lze otevřít okno grafu a okno pro sestavení protokolu.

Soubory logu a protokol jsou ukládány v adresáři programu, podadresář \Log.

*Logování AT modemu a Parametry Sítě* – logování těchto skupin je sdruženo do zaškrťovacího tlačítka „**GSM modem**“. Po zaškrtnutí se vytvoří nový log pod názvem „Modem.log“ v daném adresáři.

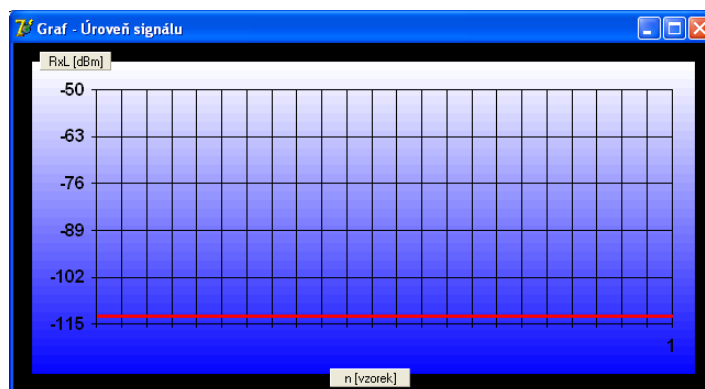
*Logování Primární Buňky* – logování skupiny je pod zaškrťovacím tlačítkem „**Primární Buňka**“. Sdružuje informace o primární buňce, kódu lokace a identifikuje BTS. Po zaškrtnutí se vytvoří nový log pod názvem „BTS.log“ v daném adresáři.

*Logování Sousedních buněk (Cells)* – logování skupiny je pod zaškrťovacím tlačítkem „**Sousední Buňky**“. Sdružuje informace uvedené v tabulce Cells. Po zaškrtnutí se vytvoří nový log pod názvem „Sousedni.log“ v daném adresáři.

*Logování AT Chat* – logování skupiny je pod zaškrťávacím tlačítkem „**AT Chat**“. Zachytává dotazy a odpovědi AT příkazů. Po zaškrtnutí se vytvoří nový log pod názvem „Chat.log“ v daném adresáři.

Pokud je požadováno průběžné logování bez smazání původních logů, je nutné mít zaškrtnuto „**Pokračuj LOG**“. Před prvním spuštěním je tlačítko zakázáno.

*Okno grafu* – tlačítko „**Graf RxL**“ vyvolává okno grafu (viz *Obrázek 2*). Okno slouží k zobrazení informačního průběhu přijímané úrovně signálu mobilním telefonem. Okno grafu lze zavřít křížkem.



*Obrázek 2 Okno Grafu – RxL*

*Okno pro vytvoření protokolu* – tlačítko „**Protokol**“ vyvolává dialogové okno (viz *Obrázek 3*) pro nastavení hlavičky protokolu. Po doplnění požadovaných údajů je možno dialog potvrdit tlačítkem „**Vytvoř**“ nebo změny stornovat křížkem. Tlačítkem „**Vytvoř**“ se sloučí logovací soubory.

*Obrázek 3 Dialogové okno protokolu*

Při použití jakéhokoliv ovládacího prvku této skupiny se aplikace pozastaví, pokud je potřeba musí se znovu spustit. Výjimkou je jen zaškrťávací tlačítko „**Pokračuj LOG**“.

## **AT Chat**

Tvoří nezávislou skupinu, kde lze testovat AT příkazy a výsledky zobrazit. Pro možnost testování je nutno mít nastavený sériový port viz podkapitola *Skupina Detekované sériové porty*. Při práci v této skupině je aplikace automaticky zastavena.

*Pole pro editaci* – do pole se zadávají příkazy AT. Podle druhu příkazu je nutno zvolit tlačítko potvrzení.

*Pole zobrazení* – zobrazí se zde veškerá komunikace na port a z portu (příkazy AT a odpovědi).

*Potvrzení* – jednotlivé tlačítka potvrzení se liší pouze potvrzovacím znakem. U tlačítka „**Proved**“ to jsou znaky #13 a #10. U „**Přeruš Ctr+Z**“ je znak #26 a u „**Enter #13**“ znak #13.

*Nastavení chování* – zaškrtačím tlačítkem „**Mazat pole**“ nastavíme automatické mazání po každém potvrzení příkazu. Zaškrtačací tlačítko „**Vypisuj OK**“ ovlivňuje výpis odpovědi. Při odmazávání nadbytečných znaků nebude smazána potvrzovací odpověď OK.

## **Spouštění**

Před spuštěním je nutno mít nastavený sériový port viz podkapitola *Skupina Detekované sériové porty*. Další nastavení není nutné lze změnit při chodu aplikace. Pozor aplikace se tím ale zastaví.

*Spouštění* – tlačítkem „**Načítej**“ se aplikace spustí a začnou se načítat jednotlivé hodnoty do daných zobrazovacích skupin. Načítání některých skupin se provádí v intervalech závislých na nastavení ve skupině *Vzorkování*.

*Zastavení* – stejným tlačítkem, ale s jiným návěstím „**Zastavit**“ lze aplikaci zastavit.

## **Zobrazované údaje**

Aplikace zobrazuje parametry sítě GSM druhé generace a identifikuje modem (mobilní přístroj). Parametry jsou zobrazeny ve skupinách.

### **GSM AT Modem**

Skupina identifikuje modem a SIM kartu přístroje. Tyto hodnoty se nemění, proto se cyklicky nenačítají.

**Parametry Sítě**

Udávají informace o operátorovi a lokalitě (LAC), kde se přístroj zrovna nachází. Zobrazení se aktualizuje každých deset cyklů (vzorku). Kód lokace se načítá každý vzorek z důvodu přidružení k následující skupině.

**Primární Buňka**

Skupina identifikuje primární buňku operátora a úroveň přijímaného signálu. Na základě kódu lokace (LAC) a kódu buňky (Cell ID) je nalezena v neoficiálních seznamech BTS. Popis se zobrazí ve skupině **Identifikována BTS**. Každý časový vzorek je prováděno načtení parametrů.

**Sousední buňky (Cells)**

Tabulka zobrazuje parametry šesti nejsilnějších sousedních buněk. Číslo kanálu, sílu signálu, NCC a BCC. Načítání hodnot se provádí každý časový vzorek, ale pouze pokud je odpověď mobilního přístroje korektní.

**Příloha 7: Datový nosič - CD**

## Souborová struktura CD

/DP_uhe026.pdf	-	diplomová práce v PDF
/Log_měření/*.log	-	logovací soubory programu ATmonGSM
/Log_měření/Protokol.log	-	výstupní protokol programu ATmonGSM
/ATmonGSMv0.9/Log	-	logovací adresář programu
/ATmonGSMv0.9/Operatori	-	adresář operátorů, obsahuje soubory *.csv
/ATmonGSMv0.9	-	adresář programu, obsahuje spustitelný soubor ATmonGSM.exe a zdrojové kódy programu v Delphi
/Install_ATmonGSM/	-	obsahuje ActiveX knihovny nutné ke spuštění